TheGreenBow VPN Certified

User Guide

Website : http://www.thegreenbow.com

Contact : support@thegreenbow.com

Table of Content

1. Presentation 4
1.1 TheGreenBow VPN Certified 2013 4
1.2. The universal VPN Client 4
1.3. Full compatibility with PKI 5
1.4. VPN security policies 5
1.5. TheGreenBow VPN Client features 5
1.6 TheGreenBow VPN Certified 2013 settings requirements 5
2. Installation 7
2.1. Installation 7
2.1.1. Installation requirements 7
2.2. Evaluation period 7
3. Activation 9
3.1. Step 1 9
3.2. Step 2 9
3.3. Activation errors 9
3.4. Manual Activation 10
3.5. Temporary license 11
3.6. Find license and software release number 12
4. Software Update 13
4.1. How to obtain an update 13
4.2. Update of VPN security policy 13
4.3. Automation 13
5. Uninstalling 14
6. Quick Use Cases 15
6.1. Opening a VPN tunnel 15
6.2. Configuring a VPN tunnel 15
6.3. Setting the automatic opening of the tunnel 15
7. Configuration Wizard 17
8. User Interface 19
8.1. Overview 19
8.2. Windows Desktop 19
8.3. Icon in Taskbar 19
8.4. Connection Panel 21
9. Configuration Panel 22
9.1. Menus 22
9.2. Status bar 23
9.3. Shortcuts 23
9.4. VPN Tunnel tree 23
9.5. "About" window 25
10. Import, Export VPN Security Policy 27
10.1. Importing a VPN security policy 27
10.2. Exporting a VPN security policy 28
10.3. Merge VPN security policies 29
10.4. Split VPN security policies 29
11. USB Mode 30
11.1. What is the USB Mode? 30
11.2. USB Mode settings 30
11.3. Use the USB Mode 33
12. Configure a VPN tunnel 34
12.1. Create a VPN tunnel 34
12.2. Configure Phase 1: Authentication 34

12.3. Configure Phase 2: IPsec 38
12.4. Configure Global Parameters....42
12.5. Save modifications....43
13. Managing Certificates (PKI Options) 44
13.1. Setup a Certificate....44
13.2. Import a certificate....47
13.3. Using Windows Certificate Store....48
13.4. Configure SmartCard or a Token....49
13.5. Use a VPN Tunnel with a Certificate from a SmarCard....49
14. 14. Remote Desktop Sharing 50
14.1. Configuring the Remote Desktop Sharing....50
14.2. Using the Remote Desktop Sharing....50
15. GINA Mode (VPN Tunnel before Windows logon) 51
15.1. Configuring the GINA Mode 51
15.2. Using the GINA Mode 52
16. Options....53
16.1. Protection et affichage (interface masquée)....53
16.2. General 54
16.3. PKI options....54
16.4. Managing languages....55
17. Security Policy Access Control....57
18. Console and Trace Mode 58
18.1. Console....58
18.2. Trace Mode....58
19. Recommendations for Security 60
19.1 Certification 60
19.2 Recommendations 60
20. FAQ....63
20.1 Questions....63
20.2 Troubleshootings....68
21. Contacts 73
22. Annex 74
22.1 Documentation reference....74
22.2 Shortcuts....74
22.3. List of available languages....74
22.4. TheGreenBow VPN Client specifications....75
22.5. Credits and Licenses....76

1. Presentation

1.1 TheGreenBow VPN Certified 2013

TheGreenBow™ VPN client is the first VPN client worldwide to achieve the Common Criteria EAL 3+ Certification NATO restricted and EU restricted agreements. This certification validates that TheGreenBow™ VPN client meets the very restrictive security standards required for use with Government agencies and strategic national operators.

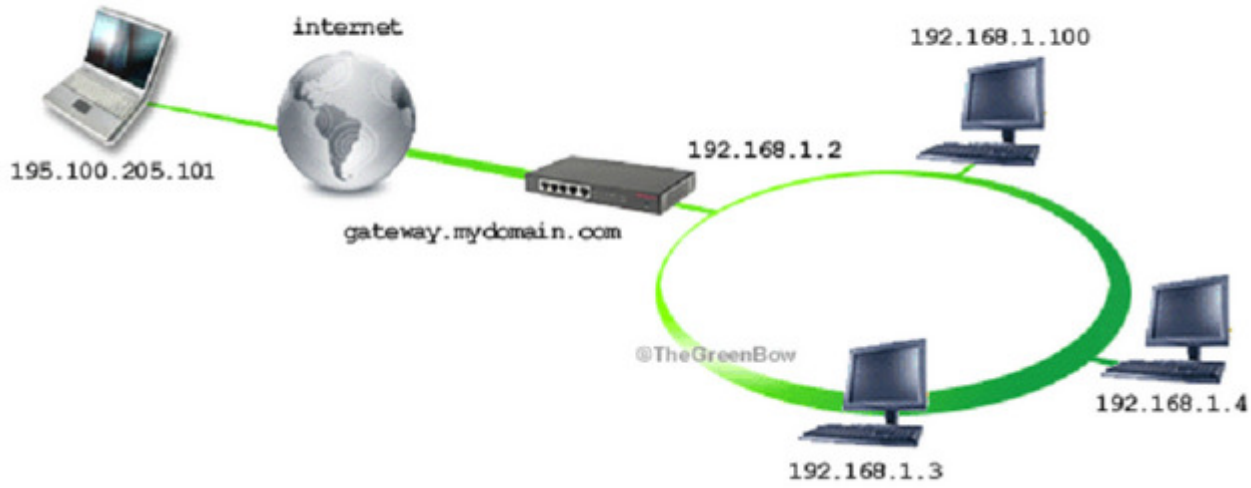
With TheGreenBow™ Certified VPN client, customers operating high-security infrastructures are enabled to establish trusted end-to-end communication channels. It is particularly suited for secure communications with personal workstations. It's the ideal solution for protecting the transmission of confidential data of strategic operators and critical infrastructures in finance, administration or defense.

With TheGreenBow™ Certified VPN client, customers operating high security infrastructures are enabled to establish trusted end communication channels. It is particularly suited for secure communications with personal workstations. It's the the transmission of confidential data of strategic operators and critical infrastructures in finance, administration or defense.

1.2. The universal VPN Client

TheGreenBow IPsec VPN Client is an IPsec VPN Client software designed for any Windows workstation or laptop. It establishes a connection, and guarantees a secure communication with the information system of the company.

TheGreenBow IPsec VPN Client is universal and compatible with all IPsec VPN gateways on the market (see the list of qualified VPN gateways). It also helps to establish VPN tunnels in point-to-point connection between two machines equipped with the software. TheGreenBow IPsec VPN Client implements IPsec and IKE standards.



For most VPN gateways on the market, TheGreenBow provides a configuration guide. To configure your VPN gateway, see this list of configuration guides of VPN gateways.

1.3. Full compatibility with PKI

TheGreenBow IPsec VPN Client is fully integrated in all PKI (Public Key Infrastructure). He brings unparalleled flexibility in taking account of certificates and smart cards:
- Compatibility with a wide range of Token and Smart Card (see list of qualified Tokens)
- Automatic detection of smart cards and tokens (in PKCS11 as CSP) or storage media (file, Windows certificate store)
- Configuring Tokens "on the fly"
- Taking into account multi-format certificates (X509, PKCS12, PEM)
- Configuring multi-criteria certificates to be used (subject, key usage, etc...).

TheGreenBow IPsec VPN Client offers more features with additional security around the PKI management, such as the opening and closing of the tunnel upon insertion and removal of the smart card, or the ability to configure the PKI interface and Smart Card in the installer software, to automate deployment.

1.4. VPN security policies

TheGreenBow IPsec VPN Client provides a high level of security management and the consideration of VPN security policies.

The software can be configured when installed to restrict all access VPN security policies the administrator only.

The software also allows you to secure the maximum use of VPN security policies, conditioning the opening of a tunnel to the various authentication mechanisms available: X-Auth, certificates...

1.5. TheGreenBow VPN Client features

TheGreenBow IPsec VPN Client provides the following features:
- Point-to-point or peer-to-gateway IPsec VPN tunnel
- VPN Tunnel on all media types: Ethernet, WiFi, 3G, satellite
- Support of PKI, and gateway or user certificate management
- Taking into account smart cards or tokens, and Windows certificate store
- User mode (limited), Director (VPN Security Policy Management) and USB (roaming)
- Open tunnel automatically and GINA mode
- X-Auth Authentication static or dynamic
- "DPD" (Dead Peer Detection) features and automatic failover the tunnel to a redundant VPN gateway
- Mechanisms for maintaining the VPN tunnel in unstable network
- IP filtering unauthorized flows (firewall feature)

See chapter "TheGreenBow VPN Client specifications".

1.6 TheGreenBow VPN Certified 2013 settings requirements

TheGreenBow VPN Certified is certified on Windows XP 32bit and Windows 7 32/64bit platforms.

The setup software (included all binary components) of the TheGreenBow VPN Certified is signed with the TheGreenBow Certificate. This enables the administrator or the user to check the integrity of the setup program.
If the software is corrupted, a Windows warning message is displayed.
The compliance of the software can be checked at any time: Right-click on the executable file, select “Properties” then select the tab “Numeric signature”.

Any user of the VPN Client software can be aware of new vulnerabilities as soon as he registers to the newsletter TheGreenBow. This registration is automatic for the software customers (i-e: a customer who provided his email address during the buying process).

Important: The user should also check the settings requirements of the TheGreenBow VPN Client.

2. Installation

2.1. Installation

Installing TheGreenBow VPN Client is done by running the program:

TheGreenBow_VPN_Client.exe

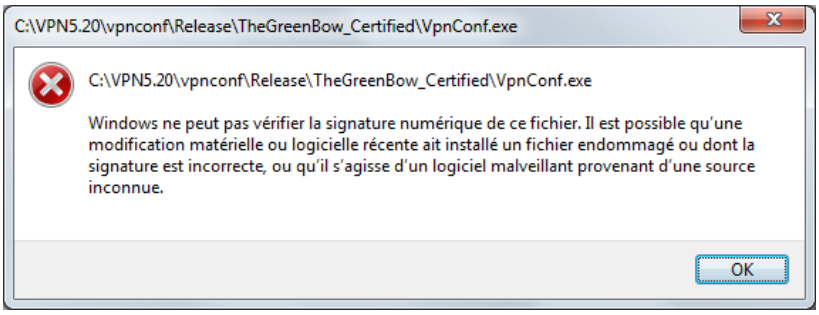
The installation is a standard procedure that requires no user input.

Note: The performance of the system is configurable using a list of command line options, or by using an initialization file. These options are described in the "Deployment Guide" i.e. tgbvpn_ug_deployment.pdf.

2.1.1. Installation requirements

See chapter specifications for supported OS.
Installation on Windows XP, Windows Vista and Windows 7 needs to be in Administrator mode the computer. When this is not the case, a warning message notifies the user and the installation stops.

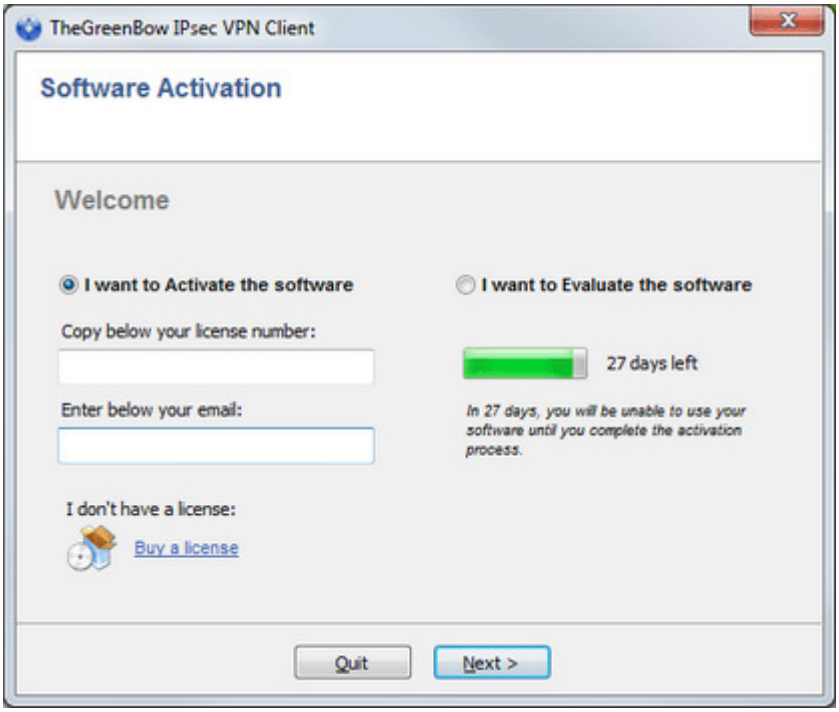
TheGreenBow VPN Certified 2013 implements an software integrity check. If the software is corrupted, it cannot start. A Windows warning message is displayed.


C:\VPN5.20\vpnconf\Release\TheGreenBow_Certified\VpnConf.exe
C:\VPN5.20\vpnconf\Release\TheGreenBow_Certified\VpnConf.exe
Windows ne peut pas vérifier la signature numérique de ce fichier. Il est possible qu'une modification matérielle ou logicielle récente ait installé un fichier endommagé ou dont la signature est incorrecte, ou qu'il s'agisse d'un logiciel malveillant provenant d'une source inconnue.
OK

2.2. Evaluation period

At its first installation on a machine, the VPN Client is in evaluation period of 30 days. During this evaluation period, the VPN Client is fully operational: all features are available.

Each launch the activation window is displayed and shows the number of days remaining evaluation.


TheGreenBow IPsec VPN Client
Software Activation
Welcome
I want to Activate the software
I want to Evaluate the software
Copy below your license number:
27 days left
Enter below your email:
In 27 days, you will be unable to use your software until you complete the activation process.
I don't have a license:
Buy a license
Quit
Next >

For further evaluation of the software, select "I want to evaluate the software" and then click "Next>".

During the evaluation period, the "About..." window displays the remaining number of days for evaluation:

During the evaluation period, it is always possible to directly access the software activation via the menu "?" > "Activation Wizard..." from the Configuration Panel.

3. Activation

VPN Client must be enabled to operate outside of the evaluation period.
The activation process is accessible either each time the software or via the menu "?" > "Activation Wizard..." from the Configuration Panel.

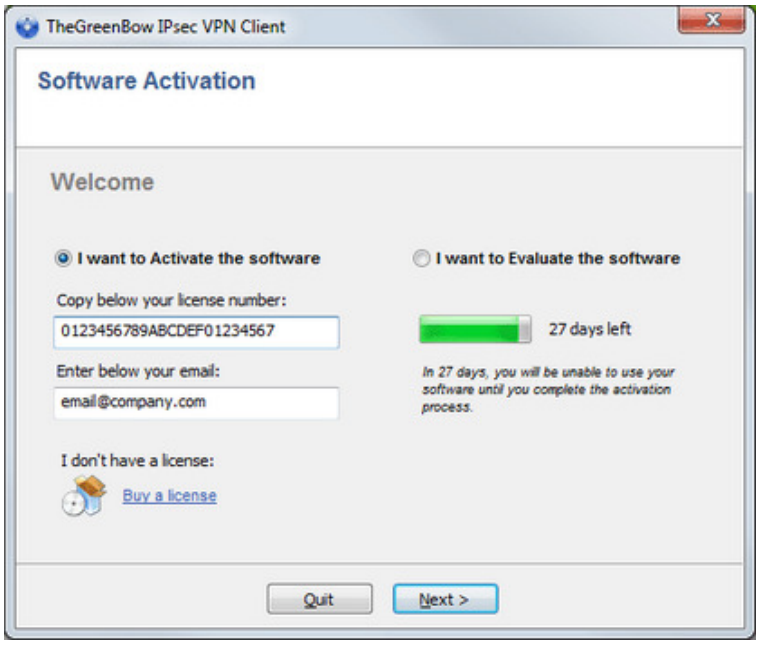
The activation process is a two-step procedure.

3.1. Step 1

Enter the license number received by email in "Copy here your license number". To get the license number, click on "Purchase license".

The license number can be copied and pasted directly from the email in the field. The license number is composed solely of characters [0 ... 9] and [A.. F], possibly grouped by 6 and separated by dashes.

Enter in the field "Enter your email address:" The email address identifying your activation. This information allows to recover in case of loss, information about your activation.


TheGreenBow IPsec VPN Client
Software Activation
Welcome
I want to Activate the software
I want to Evaluate the software
Copy below your license number:
0123456789ABCDEF01234567
27 days left
Enter below your email:
email@company.com
In 27 days, you will be unable to use your software until you complete the activation process.
I don't have a license:
Buy a license
Quit
Next >

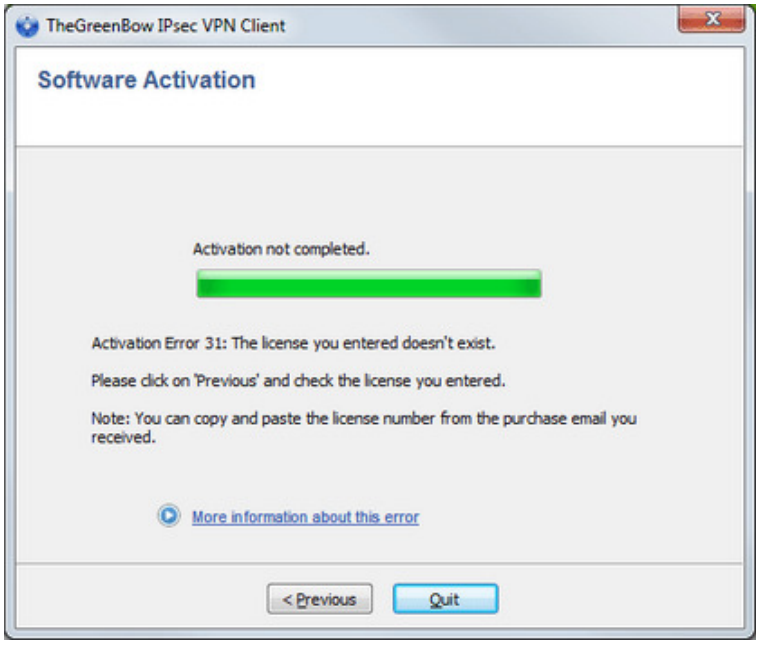
3.2. Step 2

Click "Next>", the online activation process runs automatically.
When activation succeeds, click "Start" to start the software.

Note: The software activation is linked to the computer on which the software is installed. Thus, a license number that allows only one activation can to be reused on another computer, once activated.
Also, the activation of the license number can be reset by uninstalling the software.

3.3. Activation errors

Activating the software might fail for different reasons. Each error is indicated on the activation window. It is possible that a link provides information, or offers a way to fix the problem.


TheGreenBow IPsec VPN Client
Software Activation
Activation not completed.
Activation Error 31: The license you entered doesn't exist.
Please click on 'Previous' and check the license you entered.
Note: You can copy and paste the license number from the purchase email you received.
More information about this error
< Previous
Quit

All activation errors, as well as procedures to solve the problem of activation are described on the TheGreenBow website at: www.thegreenbow.com/support_flow.html?product=vpn

Activation errors that are the most common ones include:

N°	Meaning	Resolution
31	The license number is not correct	Check the license number
33	The license number is already activated on another computer	Uninstall the computer on which the license has been activated, or contact TheGreenBow sales team
53 54	Communication with the activation server is not possible	Check the extension is connected to the Internet Check the communication is not filtered by a firewall to a proxy. If applicable, configure the firewall to let the communication, or the proxy to redirect it correctly.

3.4. Manual Activation

If you still have software activation error, it is possible to activate the software "manually" on TheGreenBow website:

① **"prodact.dat" file** — On the computer to be activated, retrieve the "prodact.dat" file located in the Windows directory "My Documents". (1)

② **Activation** — On a computer connected to the activation server (2), open the manual activation page (3), post prodact.dat file, and retrieve the tgbcode file automatically created by the server.

③ **"tgbcode" file** — Copy this "tgbcode" file in the Windows "My Documents" of the computer to activate. Launch the software: it is activated.

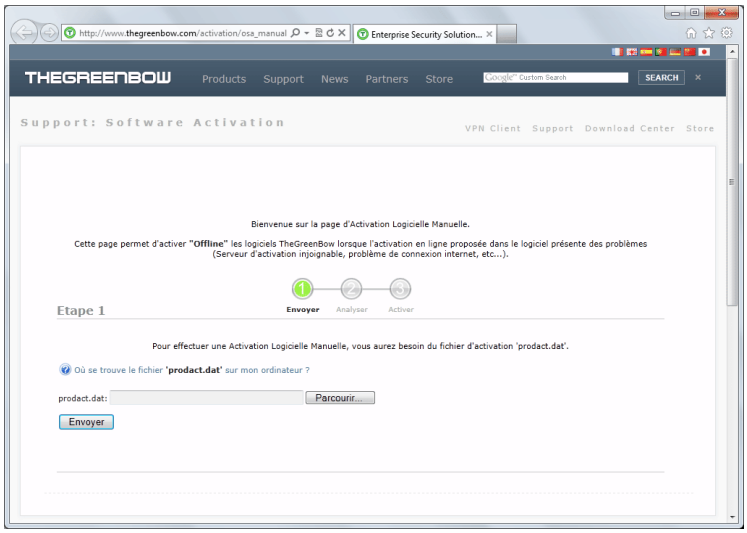
(1) The file "prodact.dat" file is a text file that contains the elements of the computer used for the activation. If this file does not exist in the "My Documents" folder, do the activation on the computer: even if it fails, it has the effect of creating this file.

(2) The activation server is TheGreenBow server available on the Internet.

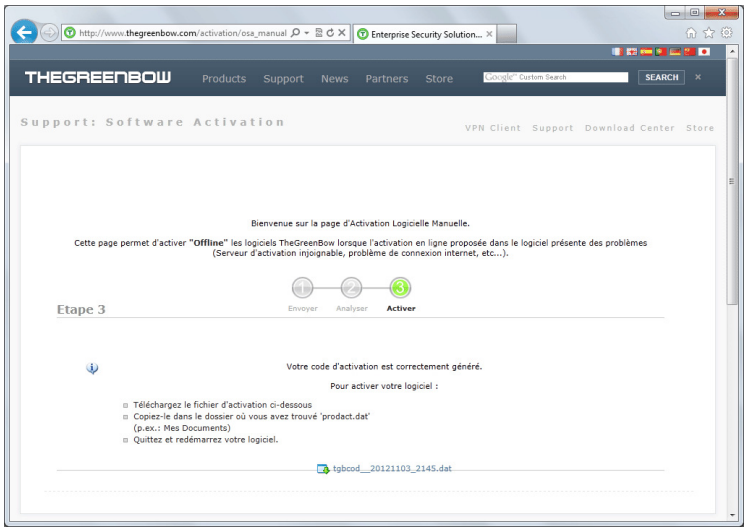
(3) See detailed procedures below.

3.4.1. Manual activation on the activation TheGreenBow server

Open the following webpage: www.thegreenbow.com/activation/osa_manual.html



Click the "Browse" button and open the "prodact.dat" file recovered on the computer to activate.
Click on "Send". The activation server verifies the validity of the product.dat file information.
Click "Perform".
During download the activation server shows the file containing the activation code used to activate the computer.

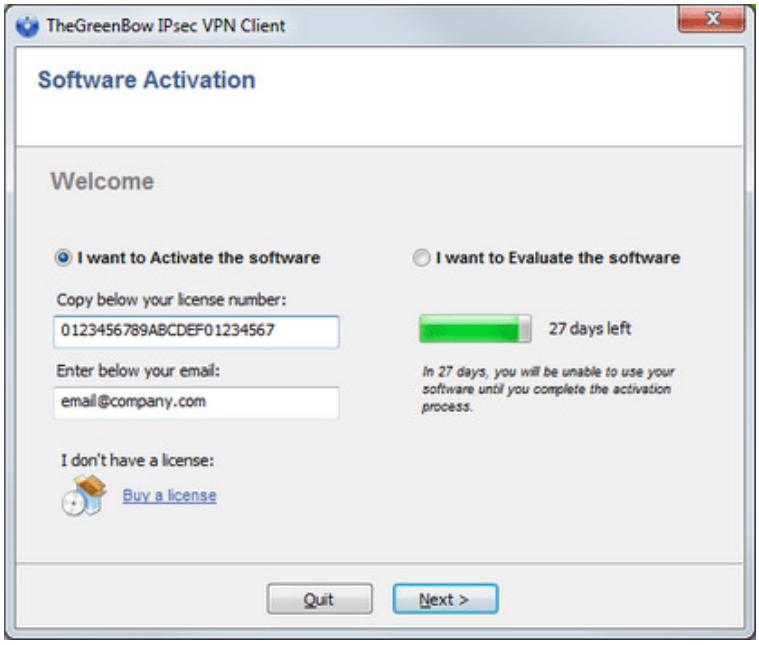


This file's name is as follow: tgbcode_[date]_[code].dat (e.g. tgbcod_20120625_1029.dat)

3.5. Temporary license

It is possible to acquire from TheGreenBow evaluation licenses, called temporary licenses, in order for example to continue testing sessions beyond the standard evaluation period. To obtain a temporary license, contact the sales department by mail: **sales@thegreenbow.com**.

During the use of a temporary license, the activation window is always displayed when the program starts. An icon identifies the license is temporary, and the number of days remaining is displayed.


TheGreenBow IPsec VPN Client
Software Activation
Welcome
I want to Activate the software
I want to Evaluate the software
Copy below your license number:
0123456789ABCDEF01234567
27 days left
Enter below your email:
email@company.com
In 27 days, you will be unable to use your software until you complete the activation process.
I don't have a license:
Buy a license
Quit
Next >

To launch the software, click on "Next>". At the end of the period of validity of the temporary license, the software must be activated by a full license for further use.

3.6. Find license and software release number

When the software is activated, the license and the email used for activation are available in the "About..." window of the software.

4. Software Update

The software allows you to check at any time if an update is available through the menu of the Configuration Panel: "?" > "Check for update".

This menu opens the checking update webpage, which indicates whether an update is available and activated, depending on the purchased type of license, as well as on the subscribed type of maintenance.

4.1. How to obtain an update

The rules to obtain a software update are as follows:

During the maintenance period (1)	I can install any updates
Outside maintenance period, or without maintenance	I can install the minor updates (2)

(1) The maintenance period starts on the first activation of the software.
(2) The minor releases (or maintenance updates) are identified by the last digit of the version, e.g. the "2" of "5.12".

Examples:
I activated the software in 5.12 release. My maintenance period has expired.
All updates from 5.13 to 5.19 releases are allowed.
Updates of 5.20 and above releases are denied.

4.2. Update of VPN security policy

During an update, the VPN security policy (VPN configuration) is automatically saved and restored.

Note: If access to the VPN security policy is locked by a password, this password is required during the update, to allow the configuration recovery.

4.3. Automation

Performing an update is configurable using a list of command line options, or by using an initialization file. These options are described in the "Deployment Guide" i.e. tgbvpn_ug_deployment.pdf.

5. Uninstalling

To uninstall TheGreenBow IPsec VPN Client:

1/ Open the Windows Control Panel
2/ Select "Add / Remove programs"

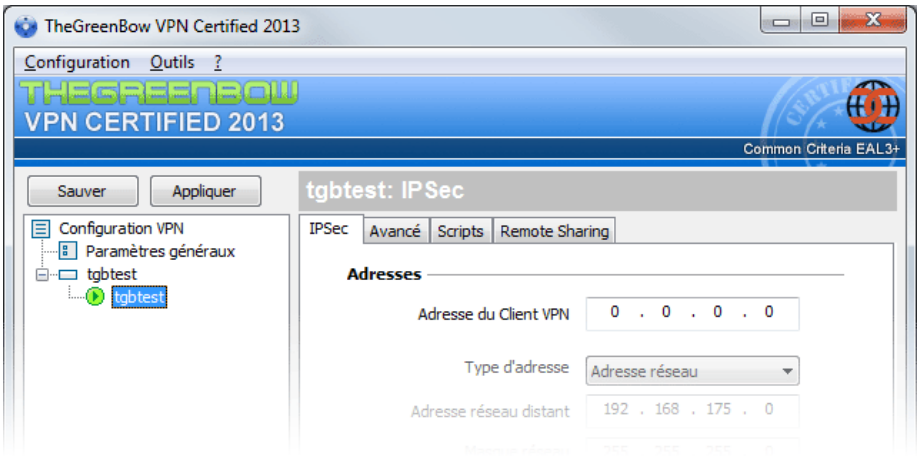
or

1/ Open Windows menu "Start"
2/ Select "Programs" > "TheGreenBow" > "TheGreenBow VPN" > "Uninstall VPN Client"

6. Quick Use Cases

6.1. Opening a VPN tunnel

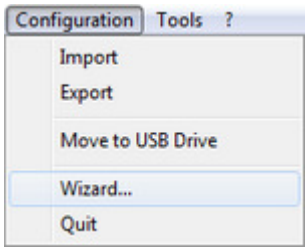
TheGreenBow IPsec VPN Client is provided with a VPN security policy for test: tgbtest
Launch the VPN Client; in the Configuration Panel, double-click the "tgbtest" tunnel in the tree as shown below:



The tunnel opens and TheGreenBow test website is automatically displayed.

6.2. Configuring a VPN tunnel

In the main interface, open the VPN Configuration Wizard: "Configuration" > "Wizard…"



Use the wizard as described in chapter "Configuration Wizard".

To complete or refine the VPN configuration, you will find many configuration guides available for most VPN gateways on the TheGreenBow website: www.thegreenbow.com/vpn/vpn_gateway.html

6.3. Setting the automatic opening of the tunnel

TheGreenBow IPsec VPN Client allows configuring a VPN tunnel so it opens automatically.

1/ A VPN tunnel can be automatically opened upon detection of traffic to the remote network.
See chapter "IPsec Advanced".

2/ A tunnel can be automatically opened upon opening (double-click) of a VPN security policy (.tgb file). See chapter "IPsec Advanced".

3/ A VPN tunnel can be automatically opened while inserting a USB drive containing the appropriate VPN security policy. See chapter "USB Mode".

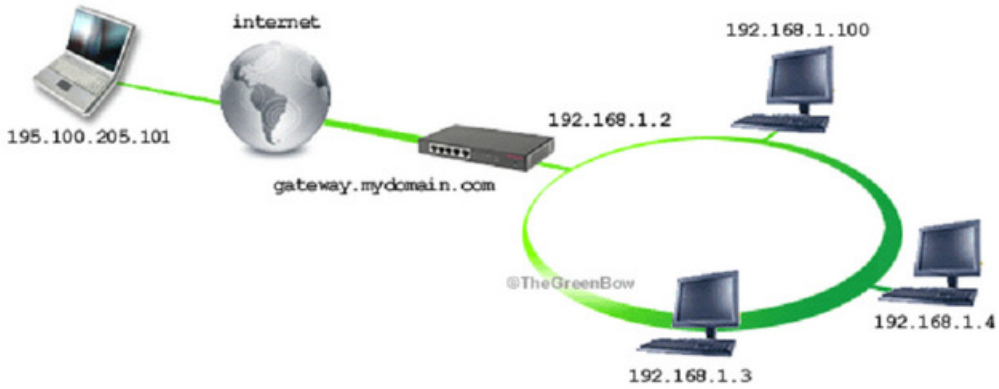
4/ A VPN tunnel can be automatically opened while inserting the Smart Card (or Token) containing the certificate used for this tunnel. See chapter "Use a VPN Tunnel with a Certificate from a SmarCard".

7. Configuration Wizard

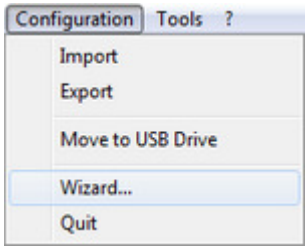
TheGreenBow VPN Client configuration wizard allows you to configure a VPN tunnel in 3 easy steps.

Using the Configuration Wizard is illustrated by the following example:

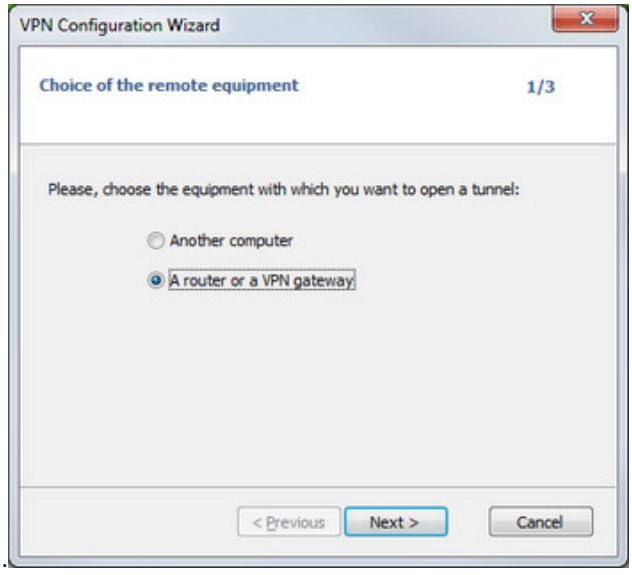
- The tunnel is opened between a computer and a VPN gateway with DNS address like "gateway.mydomain.com"
- The company's local network is 192.168.1.0 (it contains several machines with IP address such as 192.168.1.3, 192.168.1.4, etc...)
- Once the tunnel is open, the remote IP address in the corporate network will be: 192.168.1.50



In the main interface, open the VPN Configuration Wizard: "Configuration" > "Configuration Wizard".

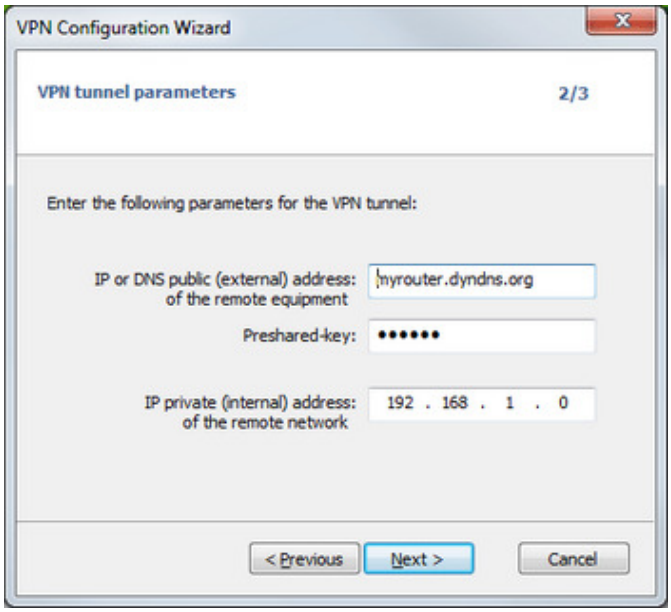


Step 1: Select the equipment at the other end of the tunnel, another computer, or (in our example) a VPN gateway


VPN Configuration Wizard
Choice of the remote equipment
1/3
Please, choose the equipment with which you want to open a tunnel:
Another computer
A router or a VPN gateway
< Previous
Next >
Cancel

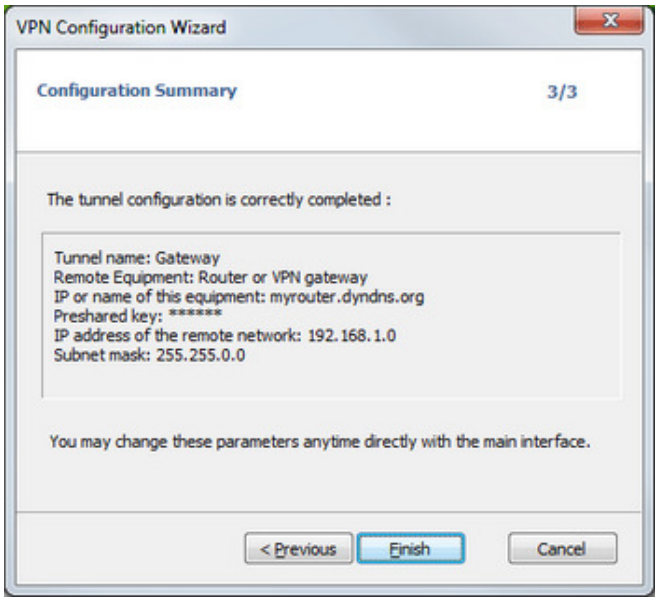
Step 2: Enter the following:

- IP or DNS address of the VPN gateway, on the Internet network side (in our example: gateway.mydomain.com)
- A Pre Shared key which must be the same on the VPN gateway
- IP address of the network (LAN) of the company (in our example 192.168.1.0)


VPN Configuration Wizard
VPN tunnel parameters
2/3
Enter the following parameters for the VPN tunnel:
IP or DNS public (external) address: of the remote equipment
myrouter.dyndns.org
Preshared-key:
IP private (internal) address: of the remote network
192 . 168 . 1 . 0
< Previous
Next >
Cancel

Click "Next>".

Step 3: Verify that the settings are correct, click "Ok".


VPN Configuration Wizard
Configuration Summary
3/3
The tunnel configuration is correctly completed :
Tunnel name: Gateway
Remote Equipment: Router or VPN gateway
IP or name of this equipment: myrouter.dyndns.org
Preshared key: ******
IP address of the remote network: 192.168.1.0
Subnet mask: 255.255.0.0
You may change these parameters anytime directly with the main interface.
< Previous
Finish
Cancel

The tunnel that has been configured appears in the Configuration tree on the Configuration Panel.
Double-click to open the tunnel, or refine the configuration using the tabs in the Configuration Panel.

For more complex configuration, or for additional information on configuring VPN gateways, visit our website: www.thegreenbow.com/vpn/vpn_gateway.html

8. User Interface

8.1. Overview

The VPN Client user interface allows:
1/ configure the software itself (boot mode, language, access control, etc...)
2/ manage security policies (VPN configuration VPN tunnels, certificate management, import, export, etc...)
3/ use VPN tunnels (opening, closing, troubleshooting, etc...)

The user interface is divided into:
- The elements of the software available on the **Windows Desktop** (desktop icons, start menu)
- An Icon in Taskbar and its associated menu
- The Connection Panel (list of VPN tunnels to open)
- The Configuration Panel

The Configuration Panel is composed of the following elements:
- A set of Menus to manage the software and VPN security policies
- The VPN Tunnel tree
- Configuration tabs for VPN tunnels
- A Status bar

8.2. Windows Desktop

8.2.1. Startup Menu

After installation, the VPN Client can be launched from the Windows Start menu.

Two links are created in the directory TheGreenBow / TheGreenBow VPN start menu:
1/ Launch TheGreenBow VPN Client
2/ Uninstall TheGreenBow VPN Client

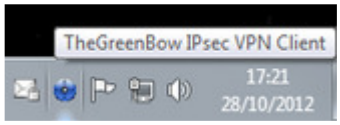
8.2.2 Desktop

During the software installation, the application icon is created on the Windows desktop.
VPN Client can be launched directly by double-clicking on this icon.

8.3. Icon in Taskbar

8.3.1. Icon

In current usage, TheGreenBow IPsec VPN Client is identified by an icon located in the taskbar.



The icon color changes if the tunnel is open:

Blue icon: no VPN tunnel is open

Green icon: at least one VPN tunnel is open

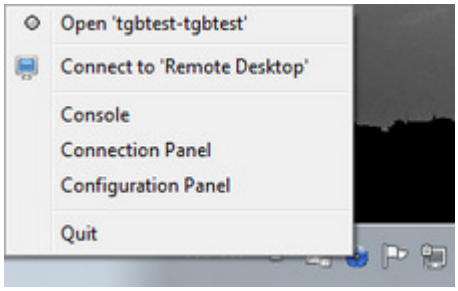
The "tooltip" the VPN Client icon indicates the status at any time of the software:

- "Tunnel <TunnelName>" if one or more tunnels are open.
- "Waiting VPN ready..." when VPN IKE is starting.
- "TheGreenBow IPsec VPN Client" when the VPN Client is launched without tunnel opened.

Left-click on the icon opens the software interface (Configuration Panel or Connection Panel).
Right-clicking the icon displays the menu associated with the icon.

8.3.2. Menu

Right click on the VPN Client icon in the taskbar displays the contextual menu associated with the icon:



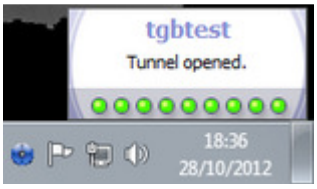
The contextual menu items are:

1/	List of VPN tunnels configured:	Click on the VPN tunnel to open or close
2/	List of remote desktop sharing sessions:	Click on a session to open or close
3/	Console:	Opens the VPN logs window
4/	Connection Panel:	Opens the Connection Panel
5/	Configuration Panel:	Open the Configuration Panel
6/	Quit:	Closes the open VPN tunnels and quit the software.

8.3.3. Taskbar popup

When opening or closing a VPN tunnel, a sliding popup window appears above the icon in the VPN taskbar. This window identifies the status of the tunnel during its opening or closing, and disappears automatically, unless the mouse is over:

Tunnel open



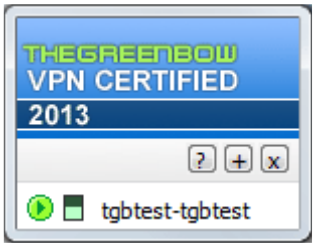
Tunnel close

Problem opening of the tunnel: the window displays brief explanation of the incident, and a clickable link to more information on this incident.

Note: The display of the popup window can be disabled in the menu "Tools" > "Options" > "View" tab, option "Don't show the systray sliding popup".

8.4. Connection Panel

Connection Panel list of VPN tunnels configured and can open or close them:



To open a VPN tunnel in Connection Panel: double-click on the VPN tunnel.

The icon to the left of the tunnel indicates its status:

- Closed tunnel
- Tunnel being opened
- Open tunnel
- Incident opening or closure of the tunnel

There is a gauge before each open tunnel. It indicates the volume of traffic exchanged in the tunnel.

The [?], [+] And [x] enables the following actions:

- [?]: Displays the "About..."
- [+]: Open the Configuration Panel
- [X] Close window

On the Connection Panel, the following shortcuts are available:

- ESC closes the window
- Ctrl+Enter opens the Configuration Panel

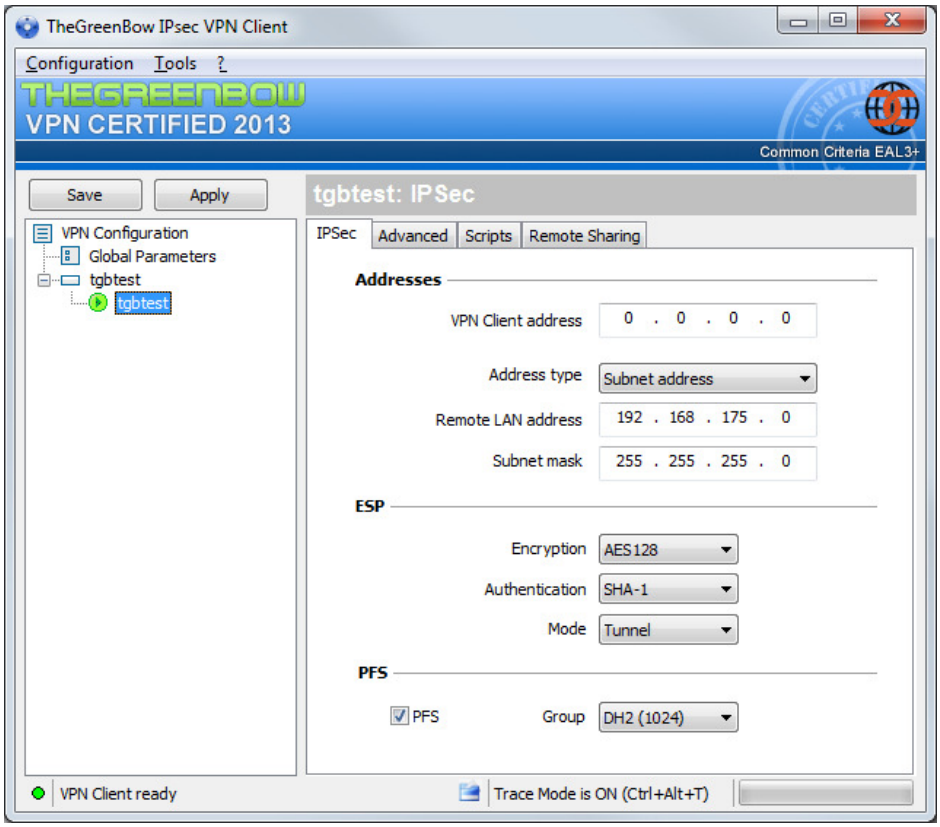
Note: Access to the Configuration Panel can be protected by a password. See chapter "Access control to the VPN security policy".

9. Configuration Panel

The Configuration Panel is the main interface of TheGreenBow VPN Client.

The Configuration Panel is composed of the following elements:

- A set of menus for managing software and VPN security policies
- The VPN tunnel tree
- Configuration tabs for VPN tunnels
- A status bar



9.1. Menus

The Configuration Panel menus are:

- "Configuration"
- Import: Importing a VPN security policy (VPN Configuration VPN)
- Export: Exporting a VPN security policy (VPN Configuration VPN)
- Move to USB drive: USB Mode settings and enable the USB mode
- Configuration Wizard
- Quit: Close the open VPN tunnels and quit the software

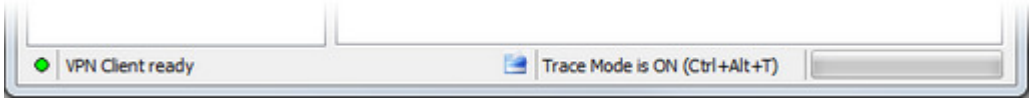
- "Tools"
- Connection Panel
- Console: IKE connection trace Window

- Reset IKE: Reboot IKE
- Options: Options protective display startup, language management, management PKI options

- "?"
- Online Support: Access to online support
- Software update: Check the availability of an update
- Buy a license online: Access to the online shop
- Activation Wizard
- "About…" window

9.2. Status bar

The status bar at the bottom of the Configuration Panel provides more information:



- The "LED" on the far left is green when all services are operational software (IKE).
- The text to the left indicates the status of the software ("VPN ready", "Save configuration", "Apply Settings", etc...)
- When enabled, tracing mode is identified in the middle of the status bar. The icon "folder" on the left blue is a clickable icon that opens the folder containing the log files generated by the mode tracing.
- The progress bar on the right of the status bar identifies the progress of the backup of Configuration.

9.3. Shortcuts

Ctrl+Enter	Toggles the Connection Panel
Ctrl+D	Opens the "Console" VPN traces
Ctrl+Alt+R	Restart IKE
Ctrl+Alt+D	Trace mode activation (generation of logs). Works also with CTRL+Alt+T

9.4. VPN Tunnel tree

9.4.1. Introduction

The left side of the Configuration Panel is the tree representation of the VPN security policy.

Each VPN tunnel is characterized by a Phase 1 and Phase 2, and Global Parameters, configurable by clicking on the first item in the tree "General Settings".

The tree can contain an unlimited number of Phase 1 and Phase 2.

Each Phase 1 can contain multiple Phase 2.

Clicking on a Phase 1 opens the configuration tabs for Phase 1 ("Configure Phase 1: Authentication").
Clicking on a Phase 2 opens the configuration tabs for Phase 2 ("Configure Phase 2: IPsec").

Double-click on a Phase 2 opens the associated VPN tunnel.

The icon to the left of the tunnel indicates its status:

- Closed tunnel
- Tunnel configured to automatically open on traffic detection
- Tunnel being opened
- Open tunnel
- Incident opening or closure of the tunnel

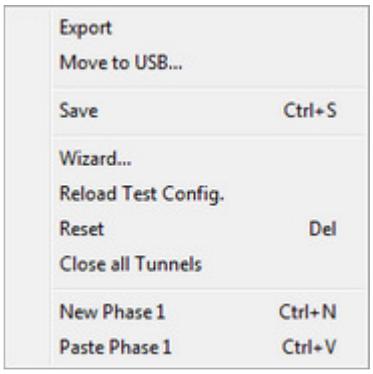
By clicking twice on a Phase 1 or a Phase 2, it is possible to edit and modify the name of the Phase.

Note: Two Phase 2 or two Phase 1 may not have the same name. If the user enters a name that is already assigned, the software displays a warning.

Unsaved changes to the VPN Configuration are identified by bold font for the Phase that changed. The tree returns to normal font when it is saved.

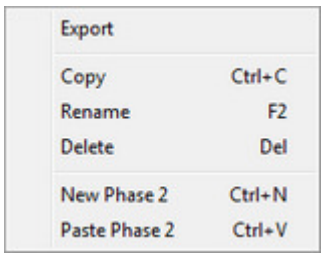
9.4.2. Contextual Menus

Right click on the VPN Configuration (root of the tree) displays the following context menu:



- Export — Exports the entire VPN security policy.
- Move USB... — Configure a USB flash drive to move in "USB mode".
- Save — Saves the VPN security policy.
- Configuration Wizard — Opens the VPN Configuration Wizard
- Reload the default configuration — TheGreenBow VPN Client is installed with a default configuration that allows to test opening a VPN tunnel. This menu allows you to reload it at any time.
- Reset — Reset the VPN security policy, subject to confirmation by the user.
- Close all tunnels — Close all open tunnels.
- New Phase1 — Adds a new Phase1 to the VPN configuration.
- Past Phase1 — Paste the previously Phase1 copied to the "clipboard".

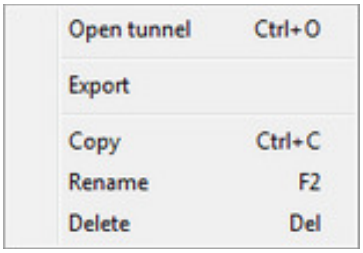
Right click on a Phase 1 displays the following contextual menu:



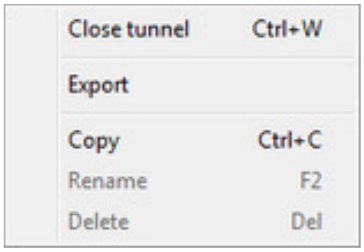
- Export — Exports the selected Phase1.
- Copy — Copies the selected Phase 1 in the "clipboard".
- Rename (1) — Allows you to rename the selected Phase 1.
- Delete (1) — Delete, the entire Phase 1, including all possible Phases 2 associated with it. This is subject to confirmation by the user.
- New Phase 2 — Adds a new Phase 2 to the selected Phase 1.
- Paste Phase 2 — Paste previously Phase 2 copied to the "clipboard" into the selected in Phase 1.

(1) This menu is disabled as long as a tunnel (Phase 2) of the selected Phase 1 is open.

Right click on a Phase 2 displays the following contextual menu:



Menu tunnel close



Menu tunnel open

- Open Tunnel — Displayed if the VPN tunnel is closed, opens the selected tunnel Phase 2.
- Close the tunnel — Displayed if the VPN tunnel is open, to close the selected tunnel Phase 2.
- Export — Exports the selected Phase 2.
- Copy — Copies the selected Phase 2.
- Rename (2) — Allows you to rename the selected Phase 2.
- Delete (2) — Delete, subject to confirmation by the user, the selected Phase 2.

(1) This feature allows you to export the entire tunnel, i.e. the associated Phase 2 and Phase 1, and to create a single VPN tunnel security policy fully operational (which can for example be imported and immediately functional).
(2) This menu is disabled until the tunnel is open.

9.4.3. Shortcuts

For the management of the tree, the following shortcuts are available:

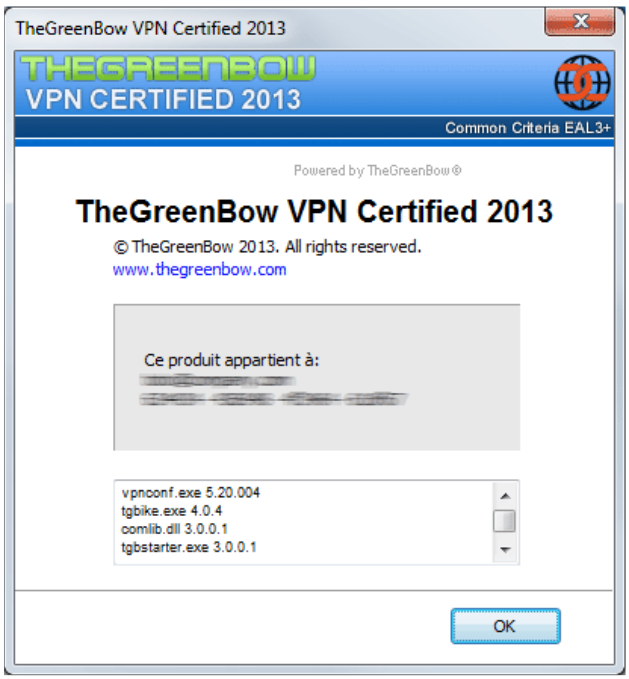
- F2: Allows you to edit the name of the selected Phase
- DEL: If a phase is selected, deletes after user confirmation.
  If the configuration is selected (root of the tree), moved the delete (reset) of the complete configuration.
- Ctrl+O: If phase 2 is selected, opens the corresponding VPN tunnel.
- Ctrl+W: If phase 2 is selected, closes the corresponding VPN tunnel.
- Ctrl+C: Copy the selected phase in the "clipboard".
- Ctrl+V: Paste (adds) the copied Phase to the "clipboard".
- Ctrl+N: Creates a new Phase 1, if the VPN Configuration is selected, or creates a new Phase 2 onto Phase 1 selected.
- Ctrl+S: Save the VPN security policy.

9.5. "About" window

The "About..." is available via:

– the menu "Help" > "About..." from the Configuration Panel,

- the system menu in the Configuration Panel,
- or via the [?] of the Connection Panel.



The "About..." provides the following information:

- The name and version of the software.
- Internet link to the TheGreenBow website.
- When the software is activated, the license number and the email used for activation.
- When the software is in evaluation period, the number of days remaining in the evaluation.
- The versions of all software components (1).

(1) It is possible to select all the contents of the list of versions (right click in the list and choose "Select All"), then copy it. It can be useful for debug purposes.

10. Import, Export VPN Security Policy

10.1. Importing a VPN security policy

TheGreenBow IPsec VPN Client can import a VPN security policy in different ways:
- From the menu "Configuration" > "Import" in the Configuration Panel
- By drag and drop of a VPN Configuration file (file ".tgb") onto the Configuration Panel
- By double-clicking a VPN Configuration file (file ".tgb")
- By using the command line option "/import" (1)

(1) In order to improve the security of the software, this function is not available with TheGreenBow VPN Certified 2013.

(2) The usage of command line options is detailed in the « VPN Client Deployment guide ». All the options available for the Security Policy import are described: «/import », « /add », « /replace » or « /importonce ».

Note: The VPN configuration files have the following extension ".tgb".

To import a VPN configuration, the user shall say if he wants to add new Configuration to the current VPN Configuration, or if he wants to replace (overwrite) the current configuration with the new VPN Configuration. If the VPN security policy has been saved with a password, it will be asked to the user.

If the VPN security policy has been exported with integrity check (see chapter "**Exporting a VPN Security Policy**") and it has been corrupted, a message alerts the user, and the software does not import the Configuration.

Note: If VPN tunnels added have the same name as the VPN tunnel in current configuration, they are automatically renamed during import (adding an increment between brackets).

Importing Global Parameters

If during import, the user selects "Replace", or if the current configuration is empty, the Global Parameters from the imported configuration replace VPN Global Parameters from the current configuration.
If during import, the user chooses "Add", Global Parameters of the current VPN configuration are kept.

Import user choice	Current configuration is empty	Current configuration not empty
Add	Global Parameters replaced by the new ones	Global Parameters kept
Replace	Global Parameters replaced by the new ones	Global Parameters replaced by the new ones

10.2. Exporting a VPN security policy

TheGreenBow IPsec VPN Client can export a VPN security policy in different ways:

- In the menu "Configuration" > "Export" from the Configuration Panel: The entire VPN security policy is exported.
- Via right click on the root of the tree of the Configuration Panel (menu choose "Export"): The entire VPN security policy is exported.
- Via right click on a Phase 1 (the menu choose "Export"): Phase 1 and all associated Phase 2 are exported
- Via right click on a Phase 2 (the menu choose "Export"): The single tunnel is exported, i.e. the selected Phase 2 and associated Phase 1.
- By using the command line option "/export" (1)

(1) The use of command line options of the software is described in the document "Deployment Guide". All the options available for exporting a VPN security policy are detailed there: "/export" or "/exportonce".

Note: The VPN configuration files have the following extension ".tgb".

Whatever the method used, the export operation begins with the choice of protection for the exported VPN security policy: It can be exported protected (encrypted) by a password, or exported "readable" (clear). When configured, the password is required from the user at the time of import.

Note: whether exported encrypted or "clear", the exported configuration integrity can be protected.

When exported VPN security policy integrity is protected, and subsequently corrupted, a warning message notifies the user during import, and the software does import the configuration (see chapter "**Importing a VPN security policy**" above).

10.3. Merge VPN security policies

It is possible to merge multiple security policies in a single VPN, by importing all VPN configurations, and selecting "Add" for each import (see chapter "**Importing a VPN security policy**").

10.4. Split VPN security policies

Using different export options (export a Phase 1 with all associated Phase 2 or export a single tunnel), it is possible to split a VPN security policy in many "sub-configurations" (See chapter "**Exporting a VPN security policy**").

This technique can be used to deploy VPN security policies on a large pool of computers: you can derive, the VPN policies associated with each computer from a common VPN policy, before distributing to each user for import.

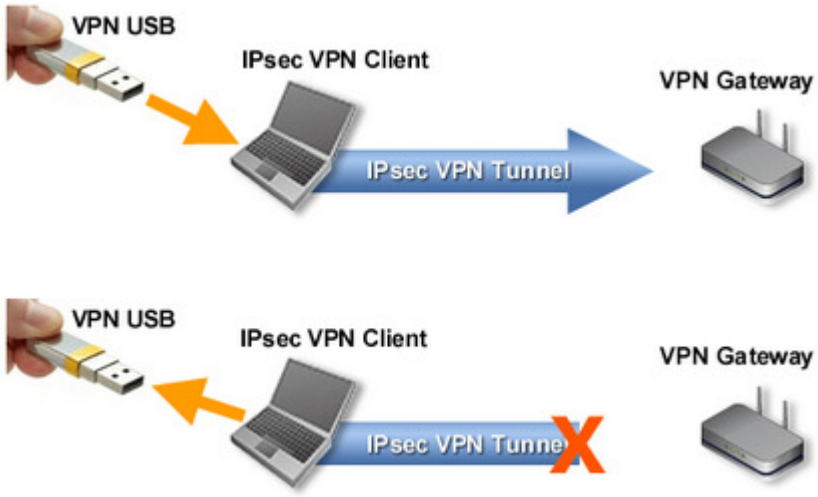
11. USB Mode

11.1. What is the USB Mode?

TheGreenBow IPsec VPN Client provides the ability to protect the VPN security policy (VPN Configuration, pre-shared key, certificate) on a USB drive.

The advantages of this mode are:

1/ The security policy is no longer stored on the computer but on a removable media (VPN Configuration stored is encrypted and protected with password)
2/ The VPN Client automatically detects USB drive containing a VPN Configuration. It will automatically load the configuration, and automatically opens the configured tunnel.
3/ When the USB drive is removed, the tunnel is automatically closed (and previous VPN Configuration restored)



In this document, the USB drive containing the VPN security policy is called "USB VPN Drive".

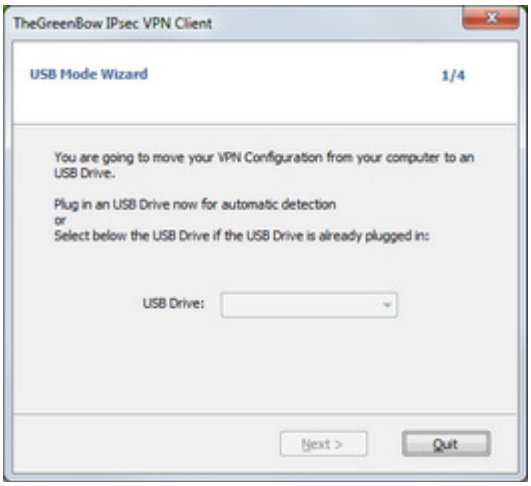
11.2. USB Mode settings

The USB mode can be configured via the setup wizard accessible via the Configuration Panel menu "Configuration" > "Move to USB drive".

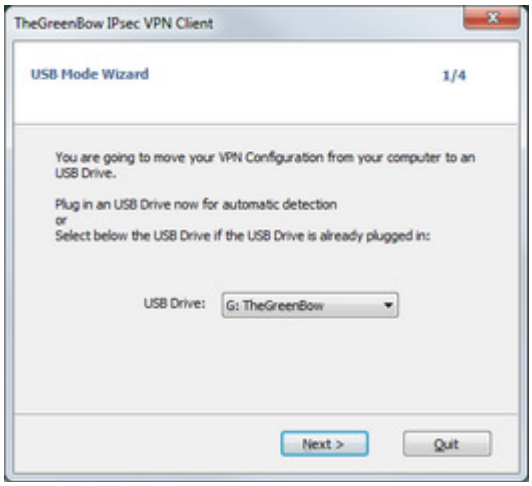
11.2.1. Step 1: Select the USB drive

Select the USB Drive to be used to protect the VPN security policy.
If a USB Drive is already plugged in, it is automatically shown in the list of USB drives available.
Otherwise, simply plug in the USB drive.

USB drive not plugged in


TheGreenBow IPsec VPN Client
USB Mode Wizard
1/4
You are going to move your VPN Configuration from your computer to an USB Drive.
Plug in an USB Drive now for automatic detection
or
Select below the USB Drive if the USB Drive is already plugged in:
USB Drive:
Next >
Quit

USB drive plugged in


TheGreenBow IPsec VPN Client
USB Mode Wizard
1/4
You are going to move your VPN Configuration from your computer to an USB Drive.
Plug in an USB Drive now for automatic detection
or
Select below the USB Drive if the USB Drive is already plugged in:
USB Drive:
G: TheGreenBow
Next >
Quit

Note: The USB mode allows the protection of a single VPN Configuration on a USB drive. If a VPN Configuration is already present on the USB drive plugged in, a warning message is displayed.

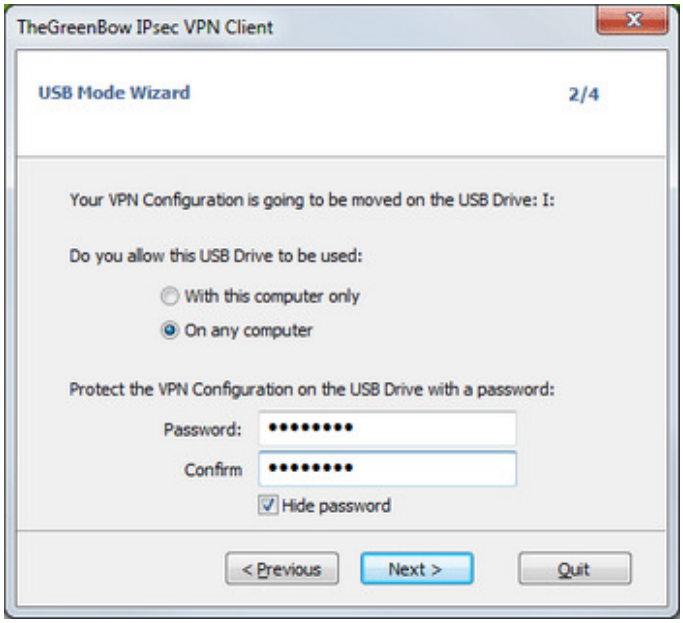
Note: When a USB drive plugged in is empty and it is the only one plugged in on the computer, the wizard automatically moves to step 2.

11.2.2. Step 2: Protection USB VPN security policy

Two protections are available:

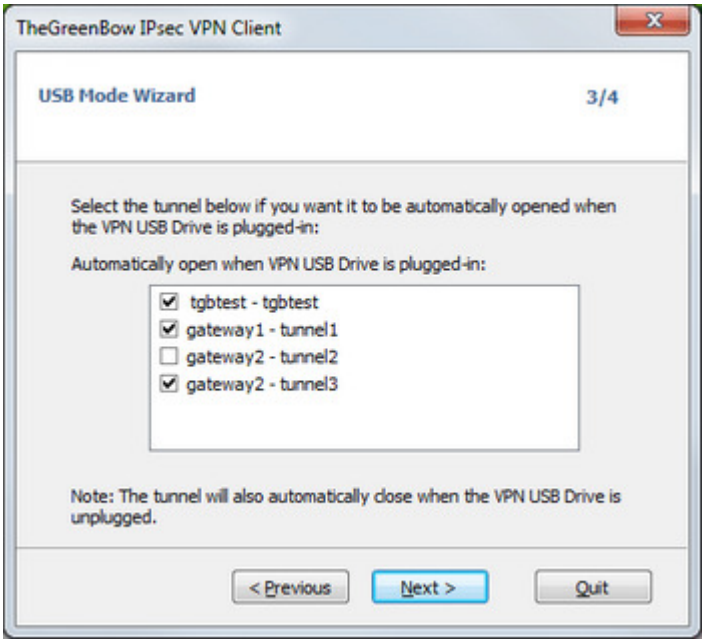
1/ Association with the current computer:
The USB VPN policy can be uniquely associated to the current computer. In this case, the USB VPN can only be used on that computer. Otherwise (the USB is not associated with a particular computer), USB VPN can be used on any computer with a VPN Client.

2/ Password protection:
The USB VPN security policy can be protected by password. In this case, the password is required each time you plug in the VPN USB drive.


TheGreenBow IPsec VPN Client
USB Mode Wizard
2/4
Your VPN Configuration is going to be moved on the USB Drive: I:
Do you allow this USB Drive to be used:
With this computer only
On any computer
Protect the VPN Configuration on the USB Drive with a password:
Password:
Confirm
Hide password
< Previous
Next >
Quit

11.2.3. Step 3: Open tunnel automatically

The wizard allows you to configure tunnels that will automatically open each time you insert the USB VPN.


TheGreenBow IPsec VPN Client
USB Mode Wizard
3/4
Select the tunnel below if you want it to be automatically opened when the VPN USB Drive is plugged-in:
Automatically open when VPN USB Drive is plugged-in:
tgbtest - tgbtest
gateway1 - tunnel1
gateway2 - tunnel2
gateway2 - tunnel3
Note: The tunnel will also automatically close when the VPN USB Drive is unplugged.
< Previous
Next >
Quit

11.2.4. Step 4: Summary

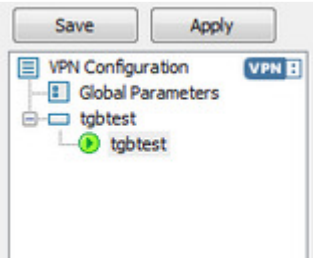
The summary is used to validate the correct setting of the USB VPN.

After validation of this last step, the VPN security policy is transferred to the USB.
It remains active as long as the USB is plugged in. Extraction of the USB VPN, VPN Client returns an empty VPN Configuration.

11.3. Use the USB Mode

When TheGreenBow IPsec VPN Client is launched, with a VPN security policy loaded or not, plug in the USB VPN. A popup window will ask to activate the USB mode.

After validation, the USB VPN policy is automatically loaded and, if applicable, tunnel(s) automatically open. The USB mode is identified in the Configuration Panel by a "USB Mode" icon at the top right of the tree.



Configuration Panel

Connection Panel

Upon USB VPN drive removal the tunnel(s) are closed, and the previous VPN policy is restored.

Note: The VPN Client takes into account only one USB VPN at a time. Other USB VPN drives are not taken into account as long as the first one is plugged in.

Note: The import feature is disabled in USB mode.

In USB mode, the USB VPN security policy can be changed. Changes to the VPN policy is saved on the USB VPN.

Note: The VPN Client does not provide a direct option to change the password and association to the computer. To change them, use the following procedure:

1/ Plug in the USB VPN drive
2/ Export VPN Configuration
3/ Remove the USB VPN drive
4/ Import VPN Configuration exported in step 2
5/ Restart Wizard USB mode with this configuration and the new desired settings.

12. Configure a VPN tunnel

12.1. Create a VPN tunnel

To create a new VPN tunnel, use the **Setup Wizard** or in the Configuration Panel tree, add a new Phase 1 and a new Phase 2 as described in chapter "**VPN Tunnel tree**".

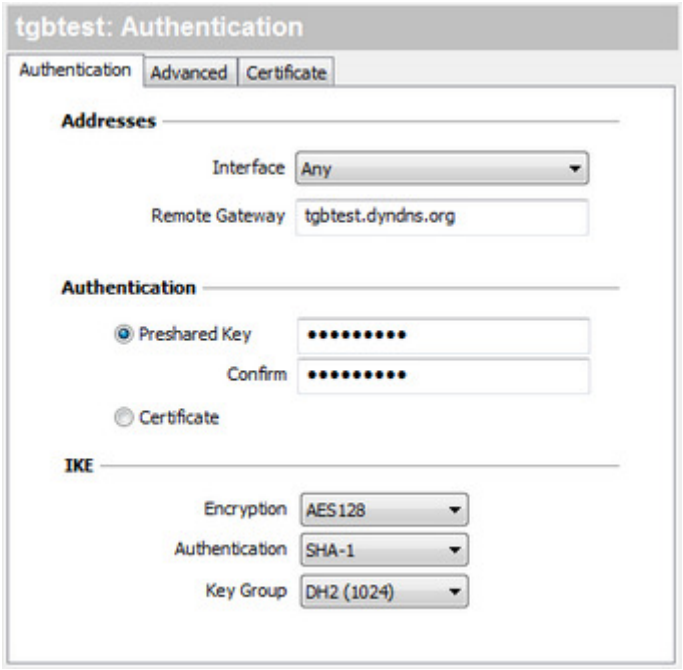
12.2. Configure Phase 1: Authentication

A VPN tunnel Phase 1 is the Authentication Phase.
Phase 1's purpose is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers. As part of Phase 1, each end system must identify and authenticate itself to the other.

To configure Phase 1, select this Phase 1 in Configuration Panel tree. Settings are configured in the tabs on the right side of the Configuration Panel.

Once setup is complete, click "Save" and then click "Apply" for this configuration to be taken into account by the VPN Client.

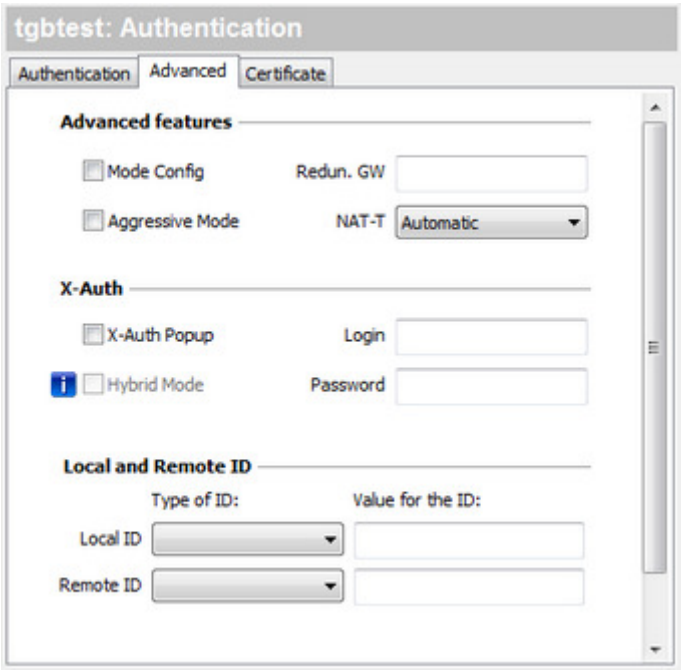
12.2.1. Authentication



Interface	IP address of the network interface of the computer, through which VPN connection is established. The VPN Client can choose this interface if you select "Any". This is useful if you are configuring a tunnel that going to be used on other computer.
Remote Gateway	IP address or DNS address of the remote gateway (in our example: gateway.mydomain.com). This field is mandatory.

Pre Shared Key	Password or key shared with the remote gateway. Note: The pre shared key is a simple way to configure a VPN tunnel. However, it provides less flexibility in the management of security than using certificates. See "Recommendations for Security".
Certificates	Use certificate for authentication of the VPN connection. Note: Using Certificate provides greater security in the management of VPN tunnel (reciprocal authentication, verification lifetimes...). See chapter "Recommendations for Security". See chapter "Managing Certificates (PKI Options)".
IKE - Encryption	Encryption algorithm used during Authentication phase: DES, 3DES, AES128, AES192, AES256. See chapter "Recommendations for Security".
IKE - Authentication	Authentication algorithm used during Authentication phase: MD5, SHA-1 and SHA-256 (i.e. SHA-2). See chapter "Recommendations for Security".
IKE – Key Group	Diffie-Hellman key length DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048) See chapter "Recommendations for Security".

12.2.2. Authentication Advanced



Mode Config	If checked, the VPN Client will activate Config-Mode for this tunnel. Config-Mode allows to the VPN Client to fetch some VPN Configuration information from the VPN gateway. See "**Mode Config**" settings below.
Redundant Gateway	This allows the VPN Client to open an IPsec tunnel with an alternate gateway in case the primary gateway is down or not responding. Enter either the IP address or the url of the Redundant Gateway (e.g. router.dyndns.com). See section "Managing Redundant Gateway" below.
Aggressive Mode	If checked, the VPN Client will used aggressive mode as negotiation mode with the remote gateway. See "Recommendations for Security" on Aggressive Mode vs. Main Mode.

NAT-T	The NAT-T mode allows Forced, Disabled and Automatic. "Disabled" prevents the VPN Client and the VPN gateway to start NAT-Traversal. "Automatic" mode leaves the VPN Gateway and VPN Client negotiate the NAT-Traversal. "Forced" mode, the VPN Client will force NAT-T by encapsulating IPsec packets into UDP frames to solve traversal with intermediate NAT routers.
X-Auth	See "Managing X-Auth" section below.
Hybrid Mode	Hybrid Mode is a mode that "blends" two types of authentication: classic VPN Gateway Authentication and X-Auth Authentication for VPN Client. To activate the Mode Hybrid, it is necessary that the tunnel is associated with a certificate (see "**Managing Certificates**"), and the X-Auth must be set. (See "Managing X-Auth" section below).
Local ID	"Local ID" is the identifier of the Authentication phase (Phase 1) that the VPN Client sends to the remote VPN gateway. Depending on the type selected, this identifier can be: – IP address (type = IP address), e.g. 195100205101 – A domain name (type = FQDN), e.g. gw.mydomain.net – Address (type = USER FQDN), e.g. support@thegreenbow.com – A string (type = KEY ID), e.g. 123456 – The subject of a certificate (type = Subject X509 (aka DER ASN1 DN)). This happens when the tunnel is associated with a user certificate (see "Managing Certificates (PKI Options)"). When this parameter is not set, the IP address of the VPN Client is used by default.
Remote ID	"Remote ID" is the identifier the VPN Client expects from the remote VPN gateway. Depending on the type selected, this identifier can be: – IP address (type = IP address), e.g. 80.2.3.4 – A domain name (type = FQDN), e.g. routeur.mondomaine.com – Address (type = USER FQDN), e.g. admin@mydomain.com – A string (type = KEY ID), e.g. 123456 – The subject of a certificate (type = DER ASN1 DN) When this parameter is not specified, the IP address of the VPN gateway is used by default.

"Mode Config"

Mode Config, when activated, allows the VPN Client to recover some parameters from the VPN gateway configuration needed to open the VPN tunnel:

- Virtual IP address of the VPN Client
- The address of a DNS server (optional)
- The address of a WINS server (optional)

Important: the VPN gateway must support the Mode Config.

When the Mode Config is not enabled, all 3 parameters "VPN Client address", "DNS Server" and "WINS Server" can be configured manually in the VPN Client (see "Phase 2 IPsec Advanced").

When the Mode Config is activated, all 3 parameters "VPN Client address", "DNS Server" and "WINS Server" are automatically filled during the opening of the VPN tunnel. Therefore they cannot be modified manually.

Managing "Redundant Gateway"

The redundant gateway algorithm is the following:

VPN Client contacts the original Gateway to open the VPN tunnel.
If the tunnel can only be opened after N retries (N: see chapter "Configure Global Parameters")
The VPN Client contacts Gateway redundant.

The same algorithm applies to the Redundant Gateway: If the redundant gateway is unavailable, the VPN Client attempts to open the VPN tunnel with the original Gateway.

Note: The VPN Client does not try to contact the redundant gateway if the original Gateway is available and there are troubles opening of the tunnel.

Note: The use of redundant gateway can be coupled with the implementation of DPD (Dead Peer Detection, see "Configure Global Parameters"). Thus, when the VPN Client detects, through the DPD, the original gateway is unavailable, it automatically switches to the redundant gateway.

Managing "X-Auth"

X-Auth is an extension of the IKE protocol (Internet Key Exchange).

X-Auth is used to force the user to enter a login and a password before the opening the VPN tunnel.

Note: This feature requires a corresponding configuration on the VPN gateway.
When the "X-Auth Popup" is selected, a window will ask the login and password to authenticate the user each time a VPN tunnel open (the window requesting the login and password has the name of the tunnel to avoid confusion).

Upon time out (configurable in "Global Parameters"), a warning message alerts the user to re-open the tunnel.

Upon incorrect login/password, a warning message alerts the user to re-open the tunnel.

VPN Client allows you to store the login and password in the X-Auth VPN security policy. This login and password are automatically sent to the VPN Gateway when the tunnel opens.

This eases the use and deployment of software. However, it is still less secure than the popup window that asks X-Auth login/password when the tunnel opens.

It is recommended to look at the chapter "Recommendations for Security".

12.2.3. Certificates

See chapter "Managing Certificates (PKI Options)".

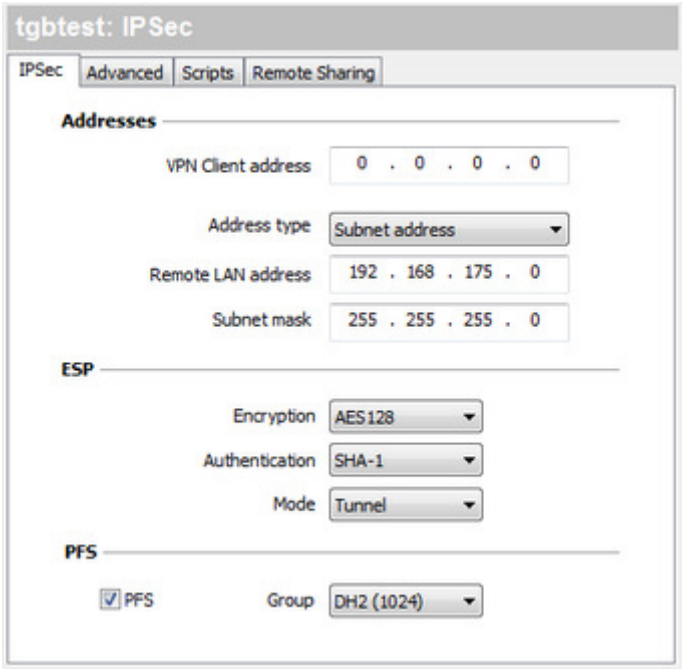
12.3. Configure Phase 2: IPsec

The purpose of Phase 2 is to negotiate the IPsec security parameters that are applied to the traffic going through tunnels negotiated during Phase 1.

To configure a Phase 2, select this Phase 2 in the Configuration Panel tree. Settings are configured in the tabs on the right side of the Configuration Panel.

After modification, click on "Save" and then click "Apply" for the configuration to be taken into account by the VPN Client.

12.3.1. IPsec

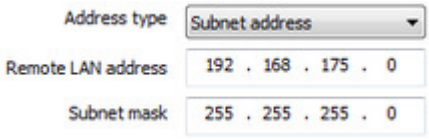


VPN Client address	This is the "virtual" IP address of the computer, as it will be "seen" on the remote network. Technically, it is the source IP address of IP packets carried in the IPsec tunnel. Note: If the Mode Config is enabled, this field is disabled. Indeed, it is automatically filled during the opening of the tunnel, with the value sent by the VPN gateway.
Address type	The remote endpoint may be a LAN or a single computer. See section "Address type configuration" below.
ESP - Encryption	Encryption algorithm negotiated during IPsec phase DES, 3DES, AES128, AES192, AES256. See "Recommendations for Security"

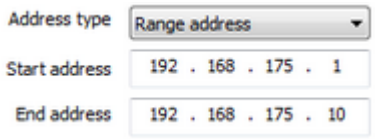
ESP - Authentication	Authentication algorithm negotiated during IPsec phase MD5, SHA-1 and SHA-256 (i.e. SHA-2) See "Recommendations for Security"
ESP - Mode	IPsec encapsulation mode: tunnel or transport. See "Recommendations for Security"
PFS - Groupe	Diffie-Hellman key length if selected DH1 (768), DH2 (1024), DH5 (1536), DH14 (2048) See "Recommendations for Security"

"Address type configuration"

If the end of the tunnel is a network, choose the "Network Address" and then set the address and mask of the remote network:



Or choose "Range Address" and set the start address and the end address:



If the end of the tunnel is a computer, select "Single Address" and set the address of the remote computer:

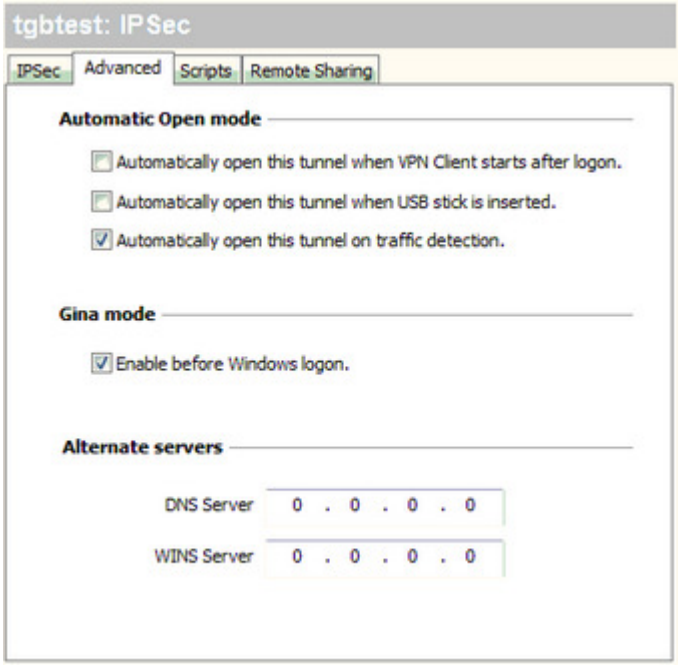
Note: The "Range Address" combined with the "Open automatically on traffic detection" allows to automatically open tunnel on traffic detection to one of the addresses in the specified address range (assuming the address range is also authorized in the configuration of the VPN gateway).

Note: If the IP address of the VPN Client is part of the IP address plan of the remote network (e.g. @IP poste = 192.168.10.2 and @remote network = 192.168.10.x), the opening of tunnel prevents the computer to contact its local network. All communications are routed within the VPN tunnel.

Configuration "all traffic through the VPN tunnel"
It is possible to configure the VPN Client to force all traffic exiting the computer passes through the VPN tunnel. To do so, select the address type "Network Address" and enter subnet mask as "0.0.0.0".

Reminder: Many configuration guides with different VPN Client VPN gateways are available on TheGreenBow website: www.thegreenbow.com/vpn/vpn_gateway.html.

12.3.2. IPsec Advanced



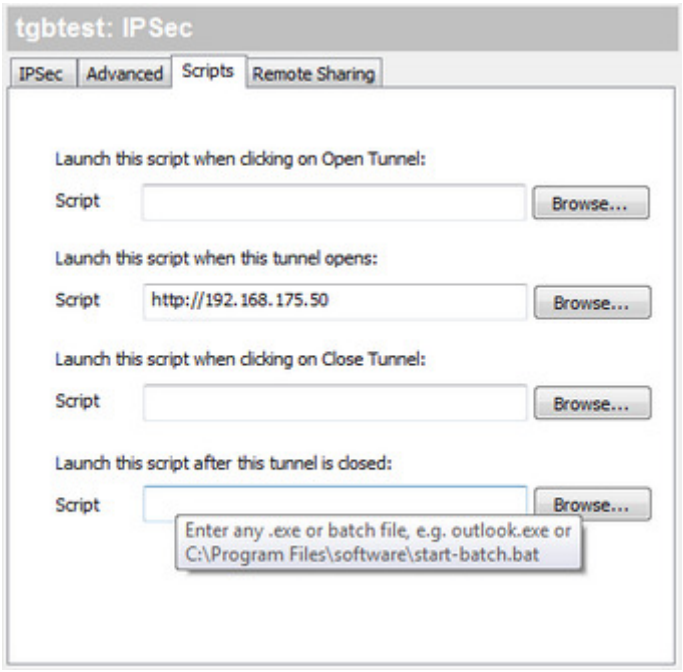
Tunnel Mode	3 modes are available for automatic opening of the tunnel: 1/ The tunnel opens automatically when the VPN Client starts (1) 2/ The tunnel is part of a configuration on USB (see "**USB mode**"), and it is opened automatically USB drive is plugged in 3/ The tunnel opens automatically on traffic detection to an IP address belonging to the remote network (see "How to configure the address of the remote network").
Gina Mode (2)	Gina opens the tunnel before Windows logon. By checking this option, the tunnel appears in the VPN Gina and can be opened before Windows logon.
Alternate servers	Input field of IP addresses of DNS and WINS servers on the remote network. Note: If the Mode Config is enabled, these fields are disabled. They are automatically filled in during the opening of the tunnel, with the values sent by the VPN gateway.

(1) This option allows you to configure to open a tunnel automatically when double-click on the file ".tgb": Select the option "Automatically open this tunnel when the VPN Client starts," save and export the configuration file "tunnel_auto.tgb" leave the VPN Client. By double-clicking on the file "tunnel_auto.tgb" VPN Client starts and the tunnel opens automatically.

(2) By extension, this option is also used to configure a tunnel to open automatically when a smart card or a token containing the certificate used by the VPN tunnel is plugged in. See chapter "Use a VPN Tunnel with a Certificate from a SmarCard".

(3) Gina Credential Providers in Windows Vista, Windows 7 and further.

12.3.3. Scripts



Scripts	Command lines can be configured to be executed: – Before opening the tunnel – After the opening of the tunnel – Before closing the tunnel – After closing the tunnel

The command line can be:

- call to a "batch" file, e.g. `"C:\vpn\batch\script.bat"`
- execution of a program, e.g. `"C:\Windows\notepad.exe"`
- opening a web page, e.g. `"http://192.168.175.50"`
- etc...

The applications are numerous:

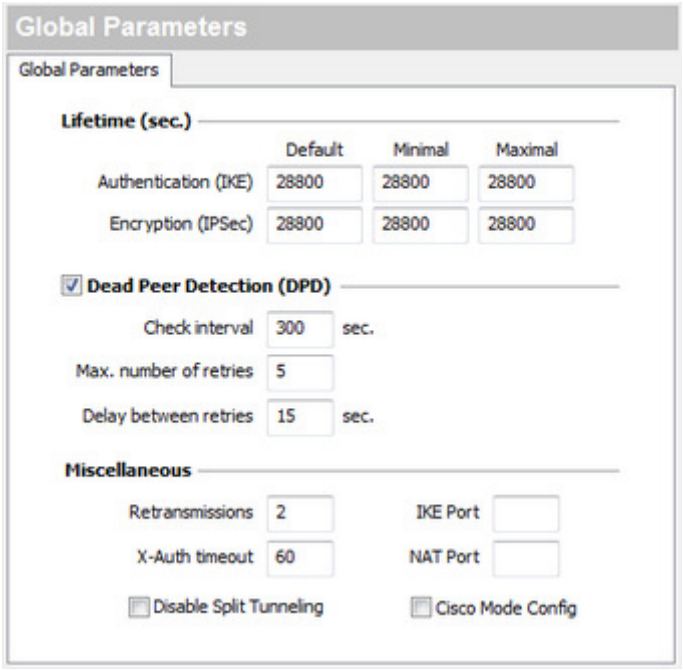
- Creating a semaphore file when the tunnel is open, so that a third-party application can detect when the tunnel is opened
- Automatic opening an intranet server, once the tunnel opens
- Cleaning or checking a configuration before the opening of the tunnel
- Check the computer (anti-virus updated, correct versioning of application, etc...) before the opening of the tunnel
- Automatic cleaning (deleting files) of a work area on the computer before closing the tunnel
- Application counting openings, closings and duration of VPN tunnel sessions
- Changing the network configuration, once the tunnel opened and restoration of the initial network configuration after closing the tunnel
- etc...

12.3.4. Remote Sharing

See chapter "Remote Desktop Sharing".

12.4. Configure Global Parameters

The Global Parameters are the parameters common to all VPN security policy (all Phase 1 and Phase 2).
After modification, click on "Save" and then click "Apply" for the policy to be taken into account by the VPN Client.



Lifetime (sec.)	Lifetimes are negotiated when tunnel opens. Each end transmits lifetime by default, and verifies that the lifetime of the other end is in the expected range (between minimum and maximum value). When lifetime expires (Phase 1 for Authentication or Phase 2 for encryption) the relevant phase is renegotiated. Lifetimes are expressed in seconds. The default values are :

	Default	Min	Max
Authentication (IKE)	3600 (1h)	360 (6min)	28800 (8h)
Encryption (IKE)	3600 (1h)	300 (5min)	28800 (8h)

DPD	DPD Feature (Dead Peer Detection) allows the VPN Client to detect that the VPN gateway becomes unreachable or inactive. (1) – Audit Period: Period between 2 DPD verification messages sent. – Number of attempts: Number of consecutive unsuccessful attempts before declaring the remote gateway unreachable – Time between attempts: Interval between DPD messages when no response is received from the VPN gateway.
Retransmissions	Number of IKE protocol messages retransmissions of before failure.
X-Auth timeout	Time to enter the login / mot de passe X-Auth

Port IKE	IKE Phase 1 exchanges (Authentication) are performed on the UDP protocol, using the default port 500. Some network devices (firewalls, routers) filter port 500. Setting of the IKE port allows to get through these filtering devices. Note: The remote VPN gateway must also be capable of performing the IKE Phase 1 exchanges on a different port than 500.
Port NAT	IKE Phase 2 exchanges (IPsec) are performed on the UDP protocol, using default port 4500. Some network devices (firewalls, routers) filter port 4500. Setting of the IKE port allows to get through these filtering devices. Note: The remote VPN gateway must also be capable of performing the IKE Phase 2 exchange on a different port than 4500.
Disable Split Tunneling	When this option is checked, only the traffic through the tunnel is allowed. (2)

(1) The DPD feature is active once the tunnel open (phase 1 open). Associated with a "Redundant Gateway", the DPD allows the VPN Client to automatically switch a gateway to another on the unavailability of one or the other.

(2) The configuration option "Disable Split Tunneling" increasing security of the computer, when the VPN tunnel is opened. In particular, this feature prevents the risk of incoming traffic that could pass through the VPN tunnel. Associated with the configuration "Force all traffic in the tunnel" (see chapter "IPsec"), this option ensures complete sealing of the computer, when the VPN tunnel is opened.

12.5. Save modifications

- Ctrl+S
- or click on "Save" then "Apply".

13. Managing Certificates (PKI Options)

TheGreenBow IPsec VPN Client is fully integrated with most PKI solution in the market.

The software implements a set of features for different certificates storage (files, Windows Certificate Store, Smart Card and Token) and a set of rules to define the certificates to use (CRL topic key usage, etc...)

TheGreenBow IPsec VPN Client supports X509 certificates.
TheGreenBow IPsec VPN Client uses the certificate files formats, PKCS12, PEM.
TheGreenBow IPsec VPN Client supports the following storage devices: Windows Certificate Store (CSP), Smart Card or Token (PKCS11 CSP).
The VPN Client supports user certificates (VPN Client side) as well as the VPN Gateway certificates.

Note: TheGreenBow VPN Client can not create certificates. However, the VPN Client can manage certificates created by third-party software, and stored on a smart card, token or in the Windows Certificate Store. VPN Client can also import certificates in the VPN security policy.

The certificate configuration is divided into three steps:
1/ "Certificate" tab of the Phase 1 involved
2/ "PKI Options" tab in the window "Tools" > "Options" in the Configuration Panel
3/ An optional startup configuration file: vpnconf.ini

13.1. Setup a Certificate

13.1.1. Select a certificate ("Certificate" tab)

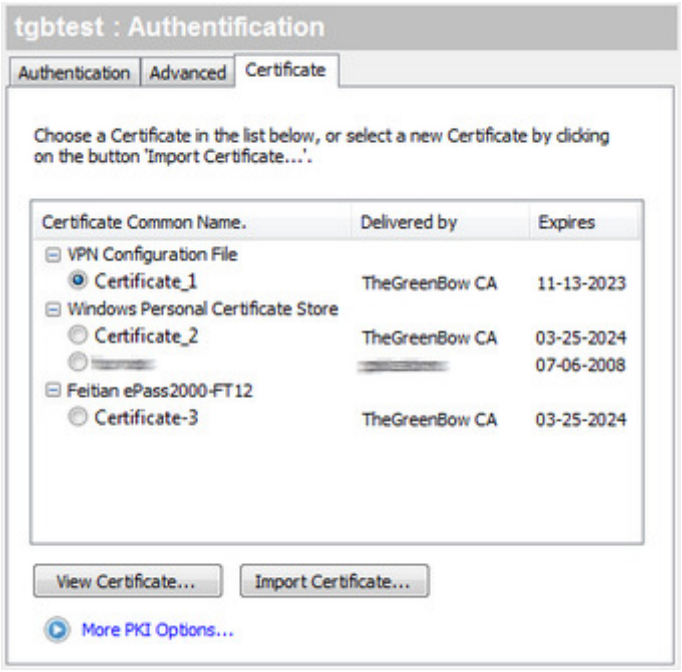
VPN Client allows you to assign a user certificate to a VPN tunnel.
There can be only one certificate per tunnel, but each tunnel can have its own certificate.

VPN Client allows you to select a certificate stored:
- In the VPN Configuration file (see "Import Certificate")
- In the Windows certificate store (see "Windows Certificate Store")
- On a smart card or a token (see "Configure a Smart Card or Token")

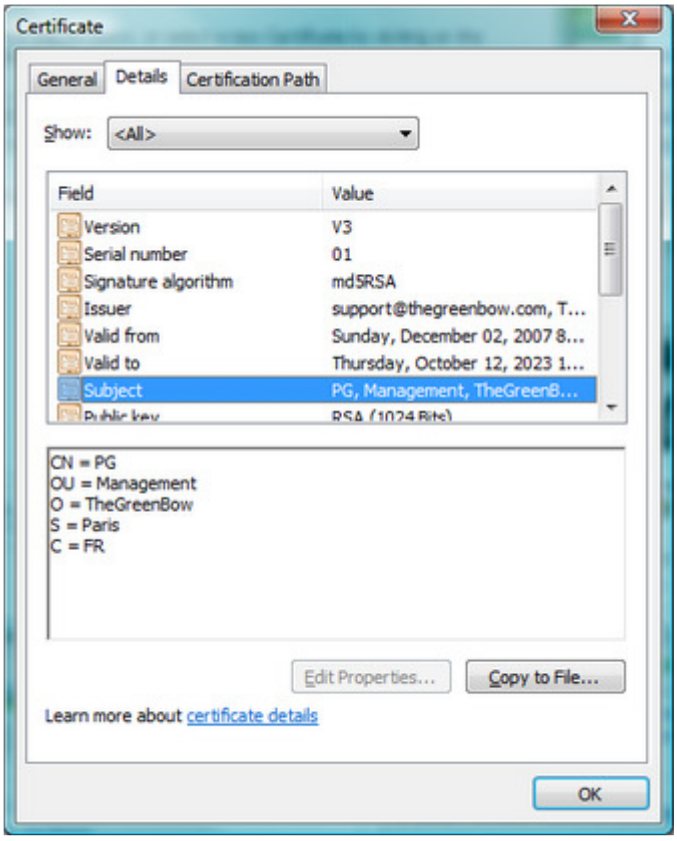
The Phase 2 "Certificate" tab lists all relevant media available on the computer, which contain certificates. If a media does not have a certificate, it is not displayed in the list (e.g. if the VPN Configuration file contains no certificate, it does not appear in the list).

By clicking one of the media, the list of certificates it contains is displayed.

Click on the desired certificate to assign to the VPN tunnel.



Once the certificate is selected, the button "View Certificate" allows to view the details of the certificate.

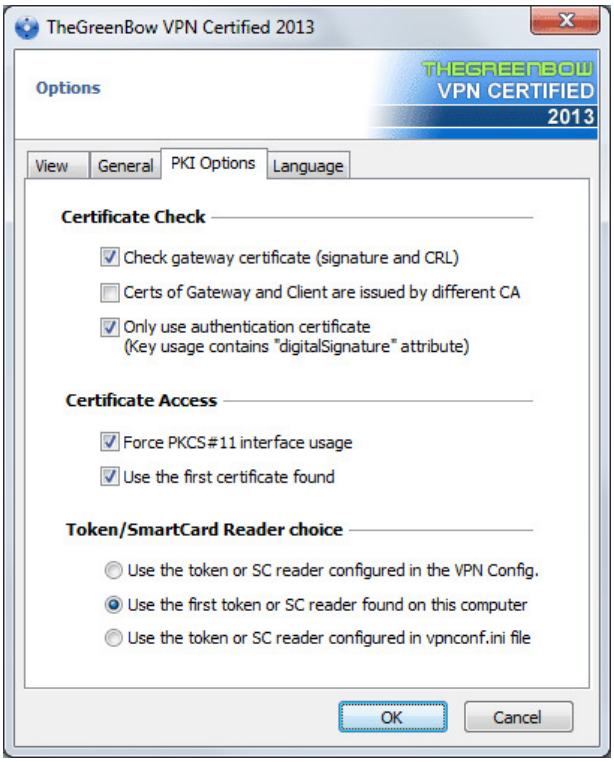


Note: Once the certificate is selected, the Phase 1 type of Local ID will automatically switch to "Subject X509" (aka DER ASN1 DN), and the certificate subject is used as the default value of this "Local ID".

13.1.2. Rules for certificate ("PKI Options" tab)

TheGreenBow IPsec VPN Client offers many possibilities to define the certificate to use, as well as smart cards or tokens.

Click on the "PKI Options" at the bottom of the "Certificates" tab or
Open the Configuration Panel menu "Tools" > "Options" and then select the "PKI Options" tab



Check Gateway Certificate	This option forces the VPN Client to check the certificate of the VPN gateway during the opening of the tunnel. The certificate expiration date is checked, as well as the signature of certificates in the certification chain and the associated CRL (certificate not revoked). See "Configuration constraints" below (1)
Gateway and Client certificate issued by different CA	If the VPN Client and Gateway use certificates from a different CA, this box must be checked (it allows the VPN Client to adapt the opening protocol of the VPN tunnel)
Only use authentication certificate	When this option is checked, only the "Authentication" Certificate type (i.e. "Key Usage" is "Digital signature") are taken into account by the VPN Client. (2)
Force PKCS#11	The VPN Client can manage PKCS11 and CSP readers. When this option is checked, the VPN Client takes into account PKCS11 readers and Token.
First Certificate found	When this option is checked, the VPN Client uses the first certificate found on the specified smart card or token, regardless of the subject of the certificate that may be configured in the Local ID field of the Phase 1 "Advanced" tab involved.
Use VPN Configuration	Smart Card or Tokens readers used are stored in the VPN Configuration. The VPN Client favors readers or Token specified in the VPN Configuration file.
Use first reader found	The VPN Client uses the first Smart Card reader or Token found on the computer to search for a certificate.

Use VpnConf.ini	The VPN Client favors the configuration file vpnconf.ini to consider smart card readers or tokens to be used. Refer to the "Deployment Guide - PKI Options" i.e. tgbvpn_ug_deployment_pki_en.pdf

(1) "Configuration constraints" for the option "VPN Gateway Certificate Verification"
Certification chain of the VPN Gateway certificate is checked. It is therefore necessary to import the root certificate and the intermediate certificates in the Windows Certificate Store.
Similarly, the CRL for the certificate of the gateway are checked. They must be available (either in the Windows Certificate Store, or downloadable)

(2) This feature allows to define a particular certificate among multiple ones, when several certificates with the same subject, for example, are stored on the same smart card or token.

13.1.3. Define a SmartCard or Token (vpnconf.ini file)

The list of Smartcard readers and Tokens compatible with TheGreenBow IPsec VPN Client is available on the TheGreenBow website at: http://www.thegreenbow.com/vpn/vpn_token.html

To install, configure and operate a smart card or a token with TheGreenBow IPsec VPN Client, see "Deployment Guide PKI Options" (tgbvpn_ug_deployment_pki_en.pdf)

Once a reader is properly installed with the smart card inserted, or when a token is available, it is identified in the list of media of certificates in the selected Phase 2 "Certificates" tab.

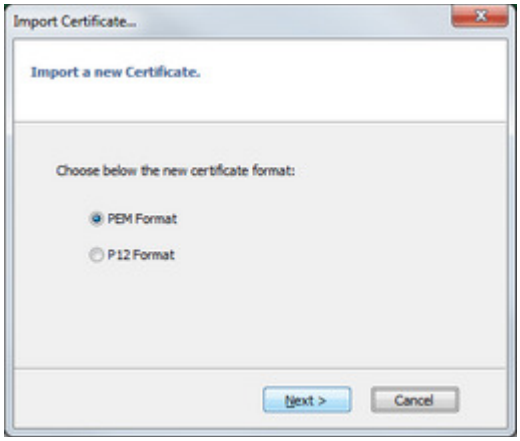
To select a certificate, click the Smart Card or Token that contains it, and select the correct certificate.

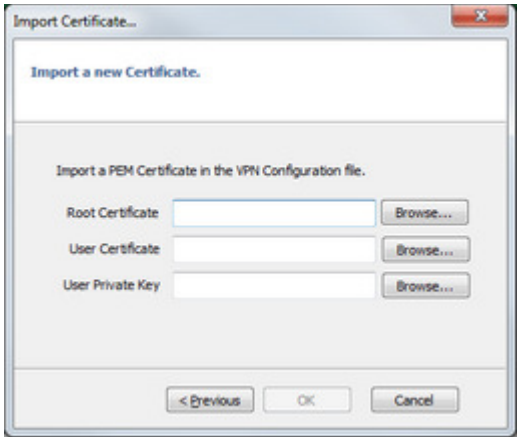
13.2. Import a certificate

TheGreenBow IPsec VPN Client can import certificates in the VPN security policy with PEM or PKCS12 format. The advantage of this solution, less secure than using the Windows certificate store or a smart card, is to enable the easy and fast deployment of certificates.

13.2.1. Import a PEM certificate

1/ In the "Certificates" tab of a Phase 2, click on "Import a Certificate..."
2/ Select "PEM Format"
3/ Select ("Browse") root certificates, user and private key to import
Note: The file with the private key must not be encrypted.
4/ Validate

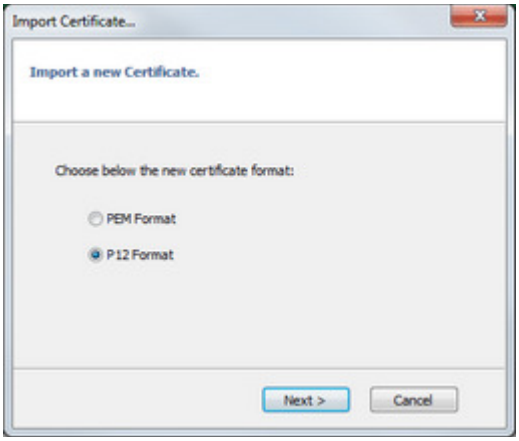


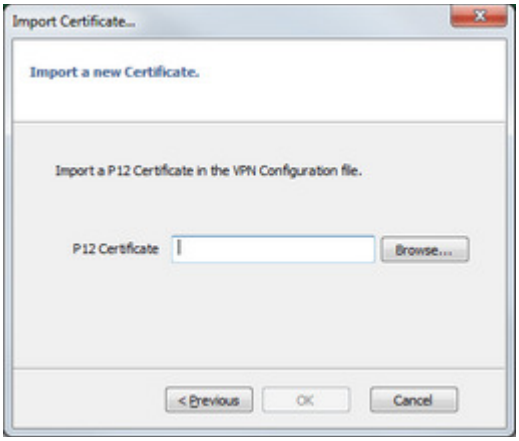


The certificate appears and is selected from the list of certificates on the "Certificate" tab.
Save the VPN security policy: The certificate is stored in the VPN security policy.

13.2.2. Import a PKCS12 certificate

1/ In the Phase 2 Certificate tab, click on "Import a Certificate..."
2/ Select "Format P12"
3/ Browse to import the PKCS12 certificate
4/ If it is protected by a password, enter the password and validate





The certificate appears and is selected from the list of certificates on the "Certificate" tab.
Save the VPN security policy: The certificate is stored in the VPN security policy.

13.3. Using Windows Certificate Store

For a certificate of Windows Certificate Store to be identified by the VPN Client, it must meet the following specifications:

- The certificate must be certified by a certification authority (excluding the self-signed certificates)
- The certificate must be located in the Certificates store "Personal" (It represents the personal identity of the user who wants to open a VPN tunnel to the corporate network).

Note: To manage certificates in the Windows Certificate Store, Microsoft offers a standard management tool "certmgr.msc." To run this tool, go to the Windows menu "Start," then in the "Search programs and files", enter "certmgr.msc."

13.4. Configure SmartCard or a Token

To install, configure and operate a smart card or a token with TheGreenBow IPsec VPN Client, see "Deployment Guide PKI Options" (tgbvpn_ug_deployment_pki_en.pdf).

13.5. Use a VPN Tunnel with a Certificate from a SmarCard

When a VPN tunnel is configured to use a certificate stored on smart card or token, a PIN code to access to the smart card is required to the user when tunnel opens.

If the smart card is not inserted, or if the token is not available, the tunnel does not open.
If the certificate does not fulfill the required conditions (see "Rules for certificate ("PKI Options" tab)"), the tunnel does not open.
If the PIN code entered is incorrect, the VPN Client notifies the user that has 3 consecutive attempts before locking out the Smart Card.

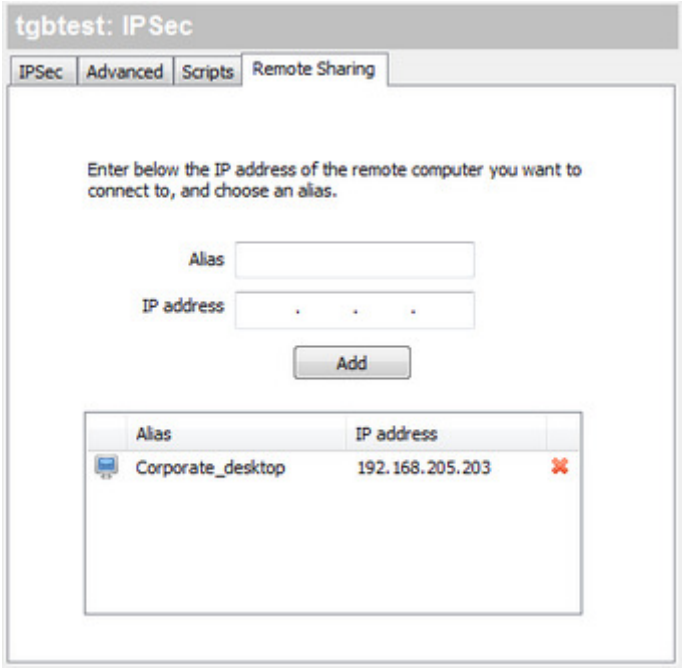
The VPN Client implements a mechanism for automatically detecting the insertion of a smart card.
Thus, the tunnels associated with the certificate contained on the smart card are opened automatically upon inserting the Smart Card. Conversely, removal of the smart card automatically closes all associated tunnels.
This functionality is achieved by checking the option "Open tunnel automatically when the USB drive is inserted" (see chapter "IPsec Advanced").

14. 14. Remote Desktop Sharing

TheGreenBow IPsec VPN Client allows to configure the "Remote Desktop" logon in the VPN tunnel with one click only: With one click, the VPN tunnel opens to the remote computer, and the RDP (Windows Remote Desktop Protocol) session is automatically opened on the remote computer.

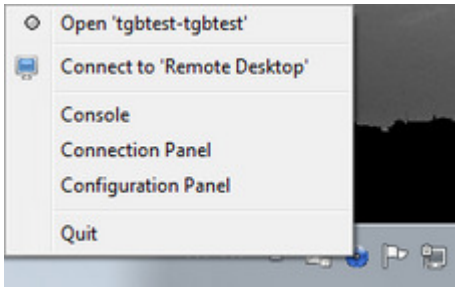
14.1. Configuring the Remote Desktop Sharing

1/ Select the VPN tunnel (Phase 2) in which the "Remote Desktop" session will be opened.
2/ Select the "Remote Sharing" tab.
3/ Enter an alias for the connection (this name is used to identify the connection in the different software menus), and enter the IP address of the remote computer.
4/ Click on "Add": The Remote Desktop Sharing session is added to the list of sessions.



14.2. Using the Remote Desktop Sharing

1/ Right click on the icon in the taskbar: the menu is displayed
2/ Click on the "Connect to Remote Desktop" in the menu in the taskbar: the VPN tunnel opens and the desktop sharing session opens.



15. GINA Mode (VPN Tunnel before Windows logon)

The GINA mode opens tunnels before Windows logon.

When a tunnel is configured in "GINA mode", a tunnel opening window similar to Connections Panel is displayed on the Windows logon screen. It allows to manually open the VPN tunnel.

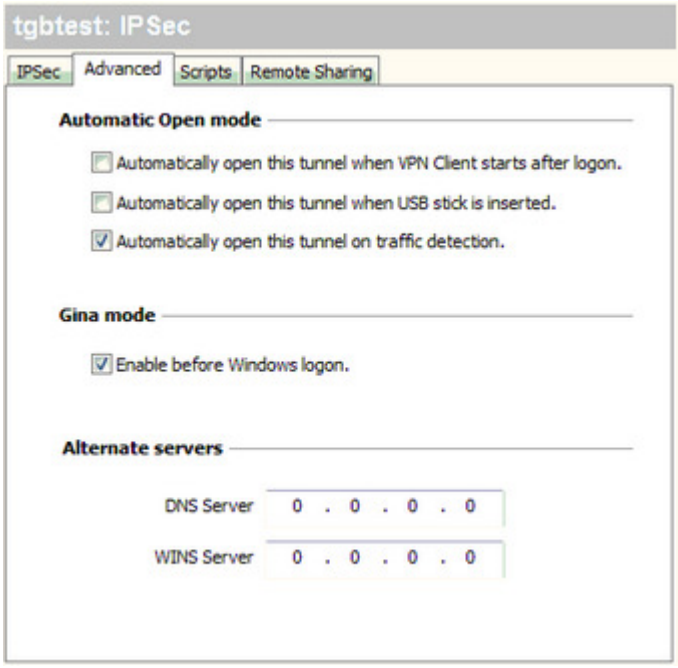
It is also possible to configure the VPN tunnel so that it automatically opens before the Windows logon

15.1. Configuring the GINA Mode

15.1.1. Manually open the VPN tunnel

1/ Select the VPN tunnel (Phase 2) in the tree view of the Configuration Panel
2/ Select the "Advanced" tab
3/ Select the option: "Gina Mode" > "Enable before the Windows logon"

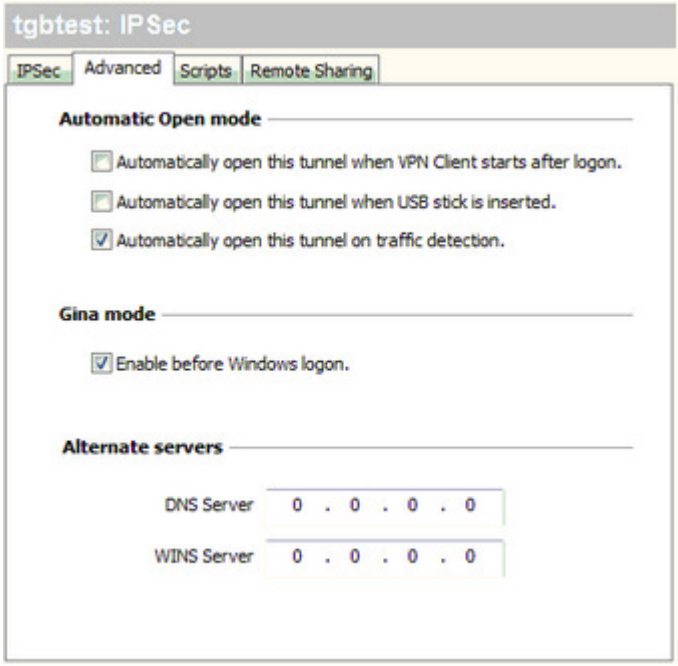
Note: An alert reminds that the script feature is not available for a tunnel in Gina mode.


tgbtest: IPSec
IPSec
Advanced
Scripts
Remote Sharing
Automatic Open mode
Automatically open this tunnel when VPN Client starts after logon.
Automatically open this tunnel when USB stick is inserted.
Automatically open this tunnel on traffic detection.
Gina mode
Enable before Windows logon.
Alternate servers
DNS Server 0 . 0 . 0 . 0
WINS Server 0 . 0 . 0 . 0

15.1.2. Automatic opening of the VPN tunnel

1/ Select the VPN tunnel (Phase 2) in the tree view of the Configuration Panel

2/ Select the "Advanced" tab
3/ Select the option: "Gina Mode" > "Enable before the Windows logon"
4/ Select the option: "Automatically open this tunnel on traffic detection"
Note: An alert reminds that the script feature is not available for a tunnel in Gina mode.



15.2. Using the GINA Mode

When the VPN tunnel is configured in GINA mode, the window of the GINA tunnels opening is displayed on the Windows logon screen. The VPN tunnel is automatically opened if configured to do so.

Note: On Windows XP, it is required to reboot the computer in order to activate the GINA Mode.

VPN Tunnel in GINA mode can perfectly implement an X-Auth Authentication (the user must then enter his login / password), or a certificate authentication (the user must then enter the PIN access code to the smart card).

Warning: If two tunnels are configured in GINA Mode, and one of them opens automatically, it is possible that both tunnels are opened automatically.

Note: In order to get the "Automatically open on traffic detection" option operational, after opening of a Windows session, the "Enable before the Windows logon" option should not be checked.

Limitation: Scripts, Config Mode and USB Mode are not available for VPN tunnels in GINA mode.

Security considerations:
A tunnel configured in GINA Mode can be opened before the Windows logon, therefore by any user of the computer. It is strongly recommended that you configure an authentication, strong whenever possible, for a tunnel in Gina Mode, e.g. an X-Auth Authentication, or preferably a certificate authentication, if possible on removable media. See chapter "Configure Phase 1: Authentication".

16. Options

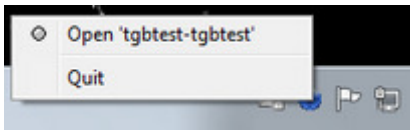
16.1. Protection et affichage (interface masquée)

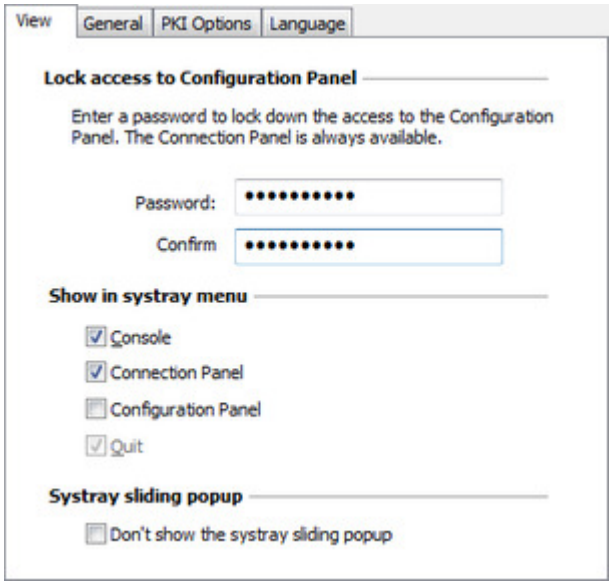
TheGreenBow VPN Client software allows to protect access to the VPN security policy by a password. From this point forward, this password is called "Administrator password".

The provided protection applies on one hand to the Configuration Panel access (regardless of which way the Configuration Panel is opened, the password is requested), on the other hand to all possible operations on the VPN security policy: changes, registration, import, export.

Thus, any import of a VPN security policy will be enabled if the right Administrator password is provided. These security options are detailed in the "Deployment Guide" document i.e. tgbvpn_ug_deployment.pdf.

The options on the "View" tab of the "Options" window also allow to hide all software interfaces, by removing from the taskbar menu the "Console", "Configuration Panel" and "Connection Panel" items. The menu in the taskbar is then reduced to the single list of available VPN tunnels.



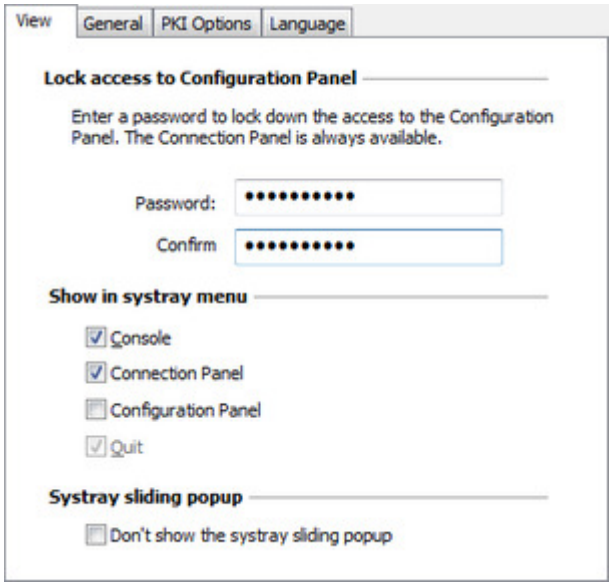


16.1.1. Access control to the VPN security policy

Any access to the VPN security policy (reading, change, application, import, export) can be protected by a password. This protection also applies to transactions done via the command line.

To ensure the integrity and confidentiality of VPN security policy, it is recommended to implement this protection.

The protection of the VPN security policy is configured via "Tools" > "Options" > "View" tab.



Note for the IT Manager: When deploying software, all these options can be preconfigured during the installation of TheGreenBow VPN Client software. These options are described in the "Deployment Guide" i.e. tgbvpn_ug_deployment.pdf.

The "Exit" item from the taskbar menu cannot be removed via software. However, it may be removed using the installation options (see "Deployment Guide" i.e. tgbvpn_ug_deployment.pdf).

16.2. General

16.2.1. Start mode

When the "Start the VPN Client after Windows logon" option is checked, the VPN Client starts automatically when Windows starts, after the Windows logon.

If the option is unchecked, the user must manually start the VPN Client, either by double-clicking on the desktop icon, or by selecting the start menu of the software in the Windows "Start" menu. See chapter "**Windows Desktop**".

16.2.2. Disabling the disconnection detection

In its generic behavior the VPN Client closes the VPN tunnel (on its side), when it finds a problem communicating with the remote VPN gateway.

In unreliable local networks, prone to frequent micro-disconnections, this feature can have drawbacks (which can go up to unable to open a VPN tunnel).

By checking the "Disable disconnection detection" box, the VPN Client avoids closing tunnels when a disconnection is detected. This ensures excellent stability of the VPN tunnel, including unreliable local networks, typically wireless networks like WiFi, 3G, 4G, or satellite.

16.3. PKI options

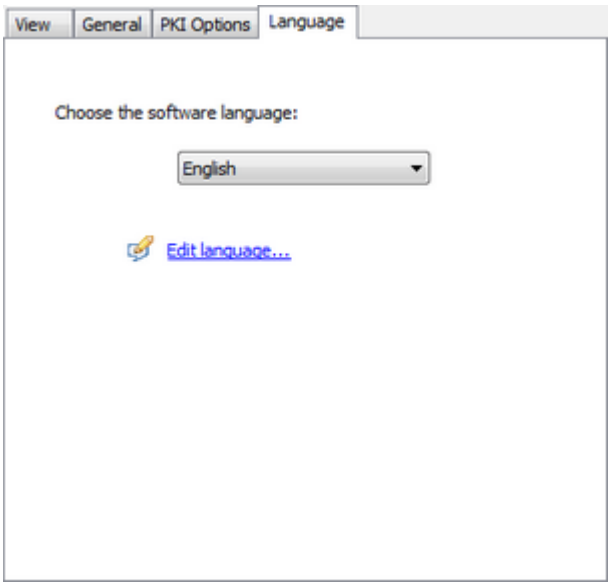
See chapter "Managing Certificates (PKI Options)".

16.4. Managing languages

16.4.1. Choosing a language

TheGreenBow IPsec VPN Client can be run in multiple languages.
It is possible to change the language while the software is running.

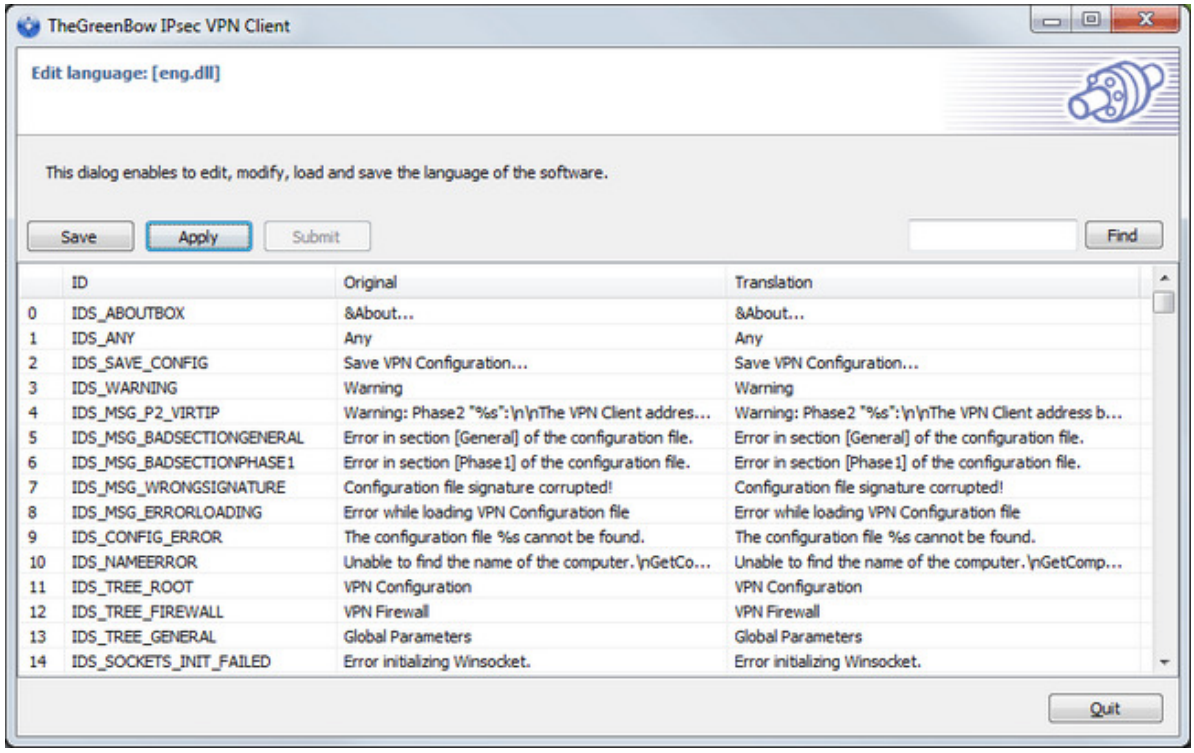
To select another language, open the "Tools" > "Options" menu and select the "Language" tab.
Choose the desired language from the proposed drop-down list:



The list of languages available as standard in the software is provided in the appendix to the chapter "List of available languages".

16.4.2. Modifying or creating a language

TheGreenBow IPsec VPN Client also allows to create a new translation or make changes to the language that is being used, then to test these changes dynamically via an integrated translation tool.
In the "Language" tab, click on the "Edit language..." link; the translation window is displayed:


TheGreenBow IPsec VPN Client
Edit language: [eng.dll]
This dialog enables to edit, modify, load and save the language of the software.
Save
Apply
Submit
Find
ID
Original
Translation
0 IDS_ABOUTBOX &About... &About...
1 IDS_ANY Any Any
2 IDS_SAVE_CONFIG Save VPN Configuration... Save VPN Configuration...
3 IDS_WARNING Warning Warning
4 IDS_MSG_P2_VIRTIP Warning: Phase2 "%s":\n\nThe VPN Client addres... Warning: Phase2 "%s":\n\nThe VPN Client address b...
5 IDS_MSG_BADSECTIONGENERAL Error in section [General] of the configuration file. Error in section [General] of the configuration file.
6 IDS_MSG_BADSECTIONPHASE1 Error in section [Phase1] of the configuration file. Error in section [Phase1] of the configuration file.
7 IDS_MSG_WRONGSIGNATURE Configuration file signature corrupted! Configuration file signature corrupted!
8 IDS_MSG_ERRORLOADING Error while loading VPN Configuration file Error while loading VPN Configuration file
9 IDS_CONFIG_ERROR The configuration file %s cannot be found. The configuration file %s cannot be found.
10 IDS_NAMEERROR Unable to find the name of the computer.\nGetCo... Unable to find the name of the computer.\nGetComp...
11 IDS_TREE_ROOT VPN Configuration VPN Configuration
12 IDS_TREE_FIREWALL VPN Firewall VPN Firewall
13 IDS_TREE_GENERAL Global Parameters Global Parameters
14 IDS_SOCKETS_INIT_FAILED Error initializing Winsocket. Error initializing Winsocket.
Quit

The translation window is divided into four columns which indicate respectively the number of the string, its ID, its translation in the original language, and its translation into the selected language.

The translation window allows:
1/ To translate each string by clicking on the corresponding line
2/ To search for a given string in any column of the table ("Search" input field, then use the "F3" key to run through all occurrences of the searched string)
3/ To save the changes ("Save" button)
Any language modified or created is saved in a "lng" file
4/ To immediately apply a change to the software: this feature allows to validate in real time whether any string is pertinent or properly displayed ("Apply" button)
5/ To send to TheGreenBow a new translation ("Send" button).

The name of the language file that is being edited is recalled in the header of the translation window.

Note: Any translation sent to TheGreenBow is published, after checking, on the TheGreenBow site, then added to the software, usually in the published official version, following receipt of the translation.

Additional notes:
Characters or following sequences of characters should not be changed during the translation:

"%s"	will be replaced by the software with a string
"%d"	will be replaced by the software with a number
"\n"	indicates a carriage return
"&"	indicates that the next character should be underlined
"%m-%d-%Y"	indicates a date format (here the format U.S.: month-day-year) modify this field only if knowledge of the format in the translated language.

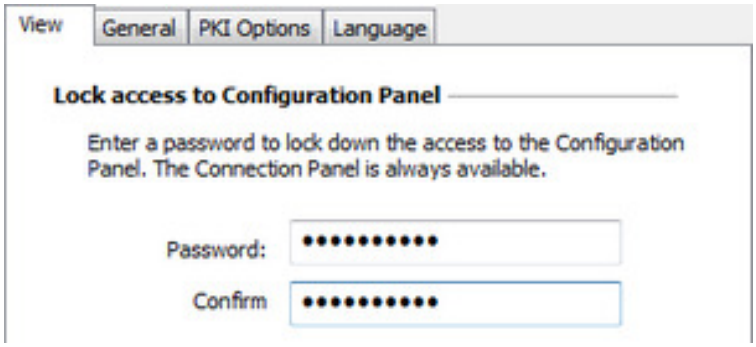
The "IDS_SC_P11_3" string must be used without modification.

17. Security Policy Access Control

Any access to the VPN security policy (read, write, apply, import, export) can be protected with a password. This protection also applies to actions carried out by the command line.

In order to ensure the integrity and confidentiality of VPN security policy, it is recommended to implement this protection.

The protection of the VPN security policy is configured via "Tools" > "Options" > "View" tab.



Once a password is configured, opening the Configuration Panel or accessing the VPN security policy (import substitution, addition) is always conditioned by entering this password:

- when the user clicks on the icon in the taskbar
- when the user selects the Configuration Panel menu in the icon menu in the taskbar
- when the user clicks on the [+] button of the Connection Panel
- when importing a new VPN security policy via the command line
- during a software update.

By combining this option with other options to limit the display of software, the administrator can configure the software in almost invisible and non-editable mode.

To remove the protection via password, empty both "Password" and "Confirm" fields, then confirm.

Note for the IT Manager: The protection of the VPN security policy can also be configured via the set up command line. This option is described in the "Deployment Guide" i.e. tgbvpn_ug_deployment.pdf.

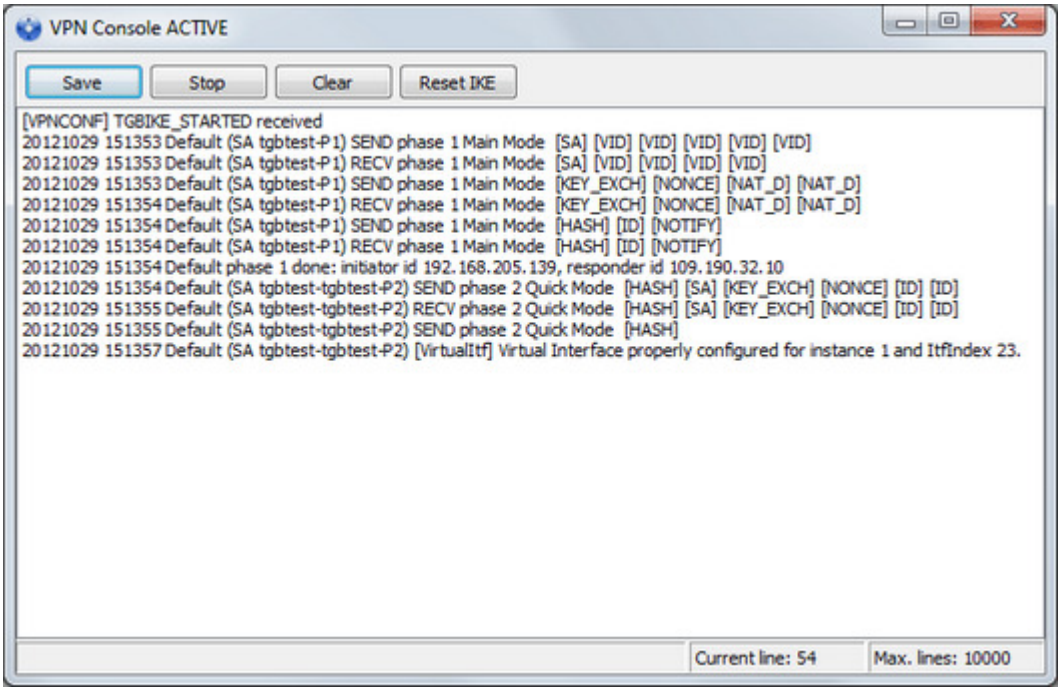
18. Console and Trace Mode

TheGreenBow IPsec VPN Client offers two tools that generate logs:
1/ The "Console" provides information and steps to open and close the tunnels (IKE messages for most of them)
2/ The "Trace Mode" asks each software component to produce its activity's log.

Both tools are designed to help the network administrator to diagnose a problem during tunnels opening, or TheGreenBow support team in identifying software's incidents.

18.1. Console

Console can be displayed as follows:
- Menu "Tools" > "Console" in the Configuration Panel
- Ctrl+D shortcut when the Configuration Panel is open
- In the software menu in the taskbar, select "Console"


VPN Console ACTIVE
Save
Stop
Clear
Reset IKE
[VPNCONF] TGBIKE_STARTED received
20121029 151353 Default (SA tgbtest-P1) SEND phase 1 Main Mode [SA] [VID] [VID] [VID] [VID] [VID]
20121029 151353 Default (SA tgbtest-P1) RECV phase 1 Main Mode [SA] [VID] [VID] [VID] [VID]
20121029 151353 Default (SA tgbtest-P1) SEND phase 1 Main Mode [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20121029 151354 Default (SA tgbtest-P1) RECV phase 1 Main Mode [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20121029 151354 Default (SA tgbtest-P1) SEND phase 1 Main Mode [HASH] [ID] [NOTIFY]
20121029 151354 Default (SA tgbtest-P1) RECV phase 1 Main Mode [HASH] [ID] [NOTIFY]
20121029 151354 Default phase 1 done: initiator id 192.168.205.139, responder id 109.190.32.10
20121029 151354 Default (SA tgbtest-tgbtest-P2) SEND phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20121029 151355 Default (SA tgbtest-tgbtest-P2) RECV phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20121029 151355 Default (SA tgbtest-tgbtest-P2) SEND phase 2 Quick Mode [HASH]
20121029 151357 Default (SA tgbtest-tgbtest-P2) [VirtualItf] Virtual Interface properly configured for instance 1 and ItfIndex 23.
Current line: 54
Max. lines: 10000

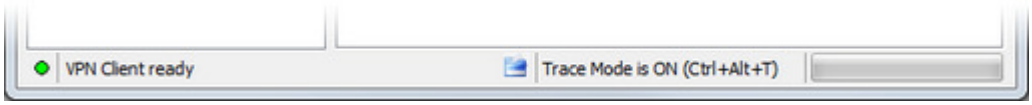
The Console features include:
- Save: Save in a file all traces displayed in the window
- Start / Stop: Start / stop the capture of recording
- Delete: Delete the content of the window
- Reset IKE: Restart the IKE service.

18.2. Trace Mode

Trace Mode is activated by the shortcut CTRL+ALT+D

Switching to Trace Mode does not require to restart the software.

When Trace Mode is enabled, each component of TheGreenBow VPN Client generates logs of its activity. The generated logs are stored in a folder accessible by clicking the blue "Folder" icon in the status bar in the Configuration Panel.



Note for the Administrator: Logs can only be activated from the Configuration Panel, which can be protected with a password.
Even if Logs don't contain sensible information, it is recommended to check – when logs or trace is activated – that logs or trace is deleted and desactivated as soon as the software is closed.

19. Recommendations for Security

19.1 Certification

TheGreenBow VPN Client Certified is the first IPsec VPN Client worldwide to achieve the Common Criteria EAL3+ Certification and to receive NATO restricted and EU restricted agreements.

TheGreenBow™ certified VPN client is certified on Windows XP 32 bit and Windows 7 32/64 bit.

19.2 Recommendations

19.2.1. General recommendations

To ensure an appropriate level of security, conditions to implement and use must be met as follows:

- The system administrator and security administrator, respectively responsible for the installation of software and the definition of VPN security policies, are considered trusted persons.
- The software user is a person trained in its use. In particular, he/she shall not disclose the information used for authentication to the encryption system.
- The VPN gateway to which the VPN Client connects allows to track the VPN activity and to show malfunctions or violations of security policies if they occur.
- The user's workstation is healthy and properly administered. It has an up-to-date anti-virus, and is protected by a firewall.
- The bi-keys and certificates used to open the VPN tunnel are generated by a trusted certification authority.

19.2.2 Host configuration

The computer on which is running the TheGreenBow VPN Client software must be clean and correctly managed.
1/ It is running an anti-virus with an updated database
2/ It is protected with a firewall. This firewall is used to control and protect incoming and outgoing communications outside the VPN Tunnels,
3/ Its operating system is updated with the latest updates, patch or service pack
4/ It is configured to avoid local attacks (memory analysis, patch or binary corruption).

Several configuration recommendations, dedicated to the security improvement of a host machine, are available on the ANSSI website:

- Guide d'hygiène informatique
- Guide de configuration
- Mises à jour de sécurité
- Mot de passe

The administrator can also check the following Microsoft documentation if he does install the software on a Windows 7 platform:
Common Criteria Security Target, Windows 7 and Windows Server 2008 R2

19.2.3 VPN Client administration

It is strongly recommended to protect access to the VPN security policy by a password and limit the visibility of the software to the end user, as detailed in chapter "Access control to the VPN security policy".

It is also recommended to set this protection at the time of installation, via the installation options described in the "Deployment Guide" i.e. tgbvpn_ug_deployment.pdf.

It is recommended to ensure that users are using the VPN Client in a "user" environment and try, as much as possible, to limit the use of the operating system with administrator rights.

It is recommended to keep the "Starting the VPN Client with Windows session" mode (after the Windows logon), which is the default installation mode.

TheGreenBow VPN Client uses the same VPN Security Policy (VPN Configuration) for all users of a multi-users platform. Thus, it is recommended to install the software on a dedicated platform, with a single-user and optionally an administrator account as described previously.

19.2.4. Configuring VPN security policy

Sensitive data in the VPN Security Policy

It is recommended to not store any sensitive data in the VPN Configuration file.

It is recommended to not use the following software functions:
1/ Do not store the login/password in the configuration (Cf chapter 12.2.2 “Phase 1 configuration / Advanced”, section “X-Auth management”)
2/ Do not import certificate in the configuration (Cf chapter 13.2 “Certificate import”) and prefer the usage of certificates stored on removable support (token) or stored in the Windows Certificate Store.
3/ Do not use the pre-shared key mode (Cf chapter 12.2.1 “Phase 1 / Authentication”) and prefer the certificate mode with certificates stred on a removable support (token) or in the Windows Certificate Store

User Authentication

The features of user authentication proposed by the VPN Client are described below, from the weakest to the strongest.

In particular, please note that authentication via pre-shared key is easy to implement, however it allows any user with access to the computer to open a tunnel without authentication check.

User Authentication Type	Strength
Pre Shared Key	weak
Static X-auth	
Dynamic X-Auth	
Certificate stored in the VPN security policy	
Certificate in the Windows Certificate Store	
Certificate on Smart Card or Token	strong

VPN Gateway Authentication

It is recommended to implement the verification of the VPN Gateway certificate, as described in chapter "Rules for certificate ("PKI Options" tab)".

IKE Protocol

It is recommended to set the "Main Mode" rather than "Aggressive Mode". See chapter "Authentication Advanced".

Mode Tunnel

It is recommended to configure the « Tunnel Mode » rather than the Transport Mode.
Cf chapter 12.3.1 “Phase 2 Configuration / IPsec”.

Gina Mode

It is recommended to add a strong authentication to any tunnel in Gina Mode.

Cryptographic algorithm and key length

In order to use the VPN Client certified software in accordance with annex B-1 of RGS 1.0, it is recommended:
1/ To choose AES128 or AES192 or AES256 as encryption IKE and ESP encryption algorithms
2/ To choose SHA-2 (SHA-256) as authentication IKE and authentication ESP algorithms
3/ To choose DH14 (2048) as IKE Key group and PFS Group.

ANSSI IPsec configuration recommendation

The recommendations above can be supplemented by the ANSSI IPsec configuration document: Recommandations de sécurité relatives à IPsec pour la protection des flux réseau

20. FAQ

This chapter details the frequently asked questions about the VPN Client. In order to get the latest version of this list, please check the following url: http://www.thegreenbow.com/vpn/support.html ("FAQ" tab)

20.1 Questions

20.1.1 Which Windows versions are supported by TheGreenBow IPsec VPN Client?

- Windows XP 32-bit. WinXP all service packs
- Windows Server 2003 32-bit
- Windows Server 2008 32/64-bit
- Windows Vista 32/64-bit
- Windows 7 32/64-bit
- Windows 8 32/64-bit
- Windows 8.1 32/64-bit

20.1.2 Releases which support old Windows versions

Windows 2000 Server	IPSec VPN Client 4.51
Windows 98	IPSec VPN Client 3.11

20.1.3 Which languages are supported?

TheGreenBow VPN Client is now available in many languages (e.g. English, French, German, Portuguese, Spanish, ...). Check our supported languages list, increasing daily, to find your language. The language can be selected during software installation of the VPN Client.

20.1.4 Which are the compatible Gateways?

TheGreenBow VPN Client is compatible with all IPSec routers compliant to the existing standards (IKE & IPsec). Check our Certified VPN Products list, increasing daily, to find your VPN gateway.

If the equipment you are looking for is not contained in this list, please contact our tech support and we will work with you to certify it. We will need configuration file, log file from "Console" window and a screenshot of the router configuration page.

20.1.5 How to connect the VPN Client to Linksys VPN router?

We've made available for download VPN Configuration Guides for most of the gateways we support on our web site support section, and there are some on Linksys. VPN Configuration Guides are either written by our partners or by our engineering team.

We do support Linksys RV082 and Linksys BEFVP41. You might want to look at our answer about Linksys WRV54G

20.1.6 How to setup TheGreenBow VPN Client using Cisco?

We've made available for download VPN Configuration Guides for most of the gateways we support on our web site, and there are some on Cisco. VPN Configuration Guides are either written by our partners or by our engineering team.

We do support Cisco gateways like Cisco PIX501, Cisco ASA 5510, Cisco PIX 506-E, Cisco 871, Cisco 1721.

20.1.7 Do you support NAT Traversal

Yes. We do support NAT Traversal Draft 1 (enhanced), Draft 2 and 3 (full implementation). IP address emulation.
Including NAT_OA support
Including NAT keepalive
Including NAT-T aggressive mode

20.1.8 Does TheGreenBow VPN Client support DNS/WINS discovering?

Yes, the VPN Client does support the "Mode-Config". "Mode-Config" is an Internet Key Exchange (IKE) extension that enables the IPSec VPN gateway to provide LAN configuration such as DNS/WINS server addresses to the remote user's machine (i.e. VPN Client). In case "Mode-Config" is not supported by remote gateway, DNS and WINS server IP addresses of the remote LAN can be defined into the VPN Client, to help users to resolve intranet addressing.

20.1.9 Is TheGreenBow VPN Client compatible with Linksys WRV54G?

TheGreenBow VPN Client is fully certified with Linksys WRV54G firmware 2.37 and later. Please download Linksys WRV54G VPN Configuration Guide.

The Linksys WRV54G firmware 2.25.2 does not accept IPSec connexions from any VPN Clients with dynamic IP addresses. However, there is a workaround. You need to set up VPN Client's IP address in the Linksys configuration. Linksys has released a newer firmware since then. You might want to test it: click here

TheGreenBow VPN Client is fully certified with Linksys RV082 and Linksys BEFVP41 (see also Certified VPN Products list or download VPN Configuration Guides).

20.1.10 Which port is needed by TheGreenBow VPN Client?

UDP port 500 and UDP port 4500 must be open and ESP protocol (protocol number 50) must be allowed.

See also other FAQs:
How to setup VPN connections and VPN ports for users in hotels or hotspots?
Unable to open a VPN tunnel under Vista, problem with Vista Firewall?
Can IKE Port be modified?

20.1.11 Is it possible to use TheGreenBow VPN Client through Microsoft ISA Server 2000 and 2004?

According from Microsoft support, in most cases, IPSec VPN traffic does not pass through ISA Server 2000.

For more details about ISA server 2004, read Q838379 in Microsoft Knowledge Base

20.1.12 What must be filled in Phase 2 field "VPN client address"?

This field is the virtual IP address that the VPN Client will have inside the remote subnet. With most of VPN gateways, this address must not belong to the remote network subnet.
For example, if you use a VPN gateway with a subnet 192.168.0.0/255.255.255.0, you should use in "VPN Client address" a value like 192.168.100.1 or 10.10.10.1.
Take the case you choose an IP address non-used in the subnet like 192.168.0.200. When the VPN Client is sending a TCP or an UDP packet to a target remote computer 192.168.0.x, this target will send inside its subnet an ARP request in order to get VPN Client MAC address and reply directly to it. But, this request cannot receive any answer because the client is not physically present inside the subnet. So, initial packets from the client will not be answered.
If your VPN gateway can answer this ARP request for the VPN Client, you can fill "VPN Client address" field with an IP address belonging to remote subnet.

You might want to download our VPN Client User Guide.

20.1.13 Is it possible to hide the graphical user interface i.e. "silent" mode?

It is possible to run the standard VPN Client setup in "silent" mode. You need to download the whole procedure described is this document: VPN Deployment Guide

20.1.14 Is TheGreenBow VPN Client compatible with Linksys WRVS4400N or WRV200?

Yes, TheGreenBow VPN Client is fully certified with Cisco Linksys WRVS4400N, Cisco Linksys WRV200 as well as Cisco Linksys RV082 and BEFVP41 (see also Certified VPN Gateway list or download VPN Configuration Guides).

20.1.15 Can a Redundant Gateway be defined?

Yes. It is possible to define a Redundant Gateway in the VPN Client. Redundant Gateway can offer to remote users a highly reliable secure connection to the corporate network. The Redundant Gateway feature allows TheGreenBow VPN Client to open an IPSec tunnel with an alternate gateway in case the primary gateway is down or not responding. Remote gateway failure is detected by "Dead Peer Detection" function.

20.1.16 Can IKE Port be modified?

Yes. A specific IKE Port can be set. To do so, go to global 'Parameters' in the Configuration Panel and enter the right port into the 'IKE Port' field and 'NAT-T port' fields.
See also other FAQs:
How to setup VPN connections and VPN ports for users in hotels or hotspots?
Unable to open a VPN tunnel under Vista, problem with Vista Firewall?

20.1.17 What are TgbStarter.exe and TgbIke.exe?

TgbStarter.exe and TgbIke.exe are components of TheGreenBow VPN Client.
TgbStarter.exe is the software daemon component (ran as a service)
TgbIke.exe is the IPSec/IKE run-time of the software.

20.1.18 The Software Activation doesn't succeed.

When I try to activate the software, it doesn't succeed (I got an error message).

You can find a complete help guide about the activation on our Online Software Activation Help Guide.

You can also get your software activated at anytime, by following the procedure described on our Manual Software activation.

20.1.19 What is the VPN Configuration for test?

A test (or demo) VPN Configuration is VPN configuration designed by TheGreenBow Techsupport team to connect to our online IPSec VPN gateways and servers. Those are always live and you can use it to test your network environement at any time. The test VPN Configuration is embedded into the VPN Client. Check out online help or download the test VPN Configuration file below.

tgbvpn_demo.tgb

20.1.20 Can I get temporary license numbers that I can use during my tests?

Yes, license can last several weeks. For further details, contact our sales team.

20.1.21 How to launch my CRM app automatically when IPSec tunnel to my corporate intranet opens?

It is possible. Go to Configuration Panel>Phase2 and click on scripts. In the Script window, you can select the application you want to start before or after a tunnel opens or closes.

20.1.22 Does VPN Client Software support two-way authentication keys and Tokens?

Yes. TheGreenBow supports several two-factor and two-way authentication Tokens to store users, personal credentials, such as private keys, passwords and digital certificates. Please see the Certified Token List.

20.1.23 How to connect to a remote Windows Domain by using the 'Enable before Windows logon' feature?

To make it work, please proceed through the following steps:

- Go to 'Phase 2' > 'Advanced' tab, select 'Enable before Windows logon'. Then click 'Save'.
- Next time, you are on the logon windows, a tiny windows will appear and will allow you to open this VPN tunnel. Several VPN Connections can be established before Windows logon.
- More info the User Guide, click on 'Search' on top left > and search for 'Gina'.

20.1.24 How to setup VPN connections and VPN ports for users in hotels or hotspots?

For more information on the negotiation of NAT Traversal in IKE see IETF RFC 3948 (UDP Encapsulation of IPsec Packets), IETF RFC 3947 (Negotiation of NAT-Traversal in the IKE) or draft "draft-ietf-ipsec-nat-t-ike-08". Also see the TCP and UDP ports list.

Here are the negotiation Phases in VPN connection and their default VPN Ports when TheGreenBow VPN Client software is behind any router:

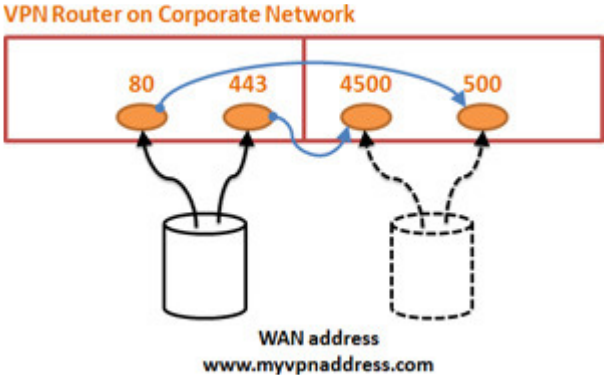
Phase	Default Port	Where to modify the ports?
Phase1 negotiation	UDP Port 500	Go to 'Config Panel' > 'Parameters' > 'IKE Port'
Phase2 negotiation	UDP Port 4500	Go to 'Config Panel' > 'Parameters' > 'NAT-T Port'
Traffic after IPSec/IKE negotiation	Stays on last port defined	

In some hotels, hotspots or airports, the UDP port 500 and 4500 for outgoing traffic might be prohibited, preventing any outgoing VPN Connections to your corporate network. So it is necessary to configure IKE and NAT-T ports accordingly.

Here is an example of alternative VPN Port in Configuration Panel (i.e. remember this only affects UDP protocol):

IKE Port	NAT-T Port
80	443

If you decide to use non default VPN Ports (i.e. UDP 500 & UDP 4500), the destination router (i.e. at the edge of your corporate network) must be configured to reroute the incoming traffic associated with the new selected VPN ports onto the default UDP 500 & UDP 4500 so that they properly routed to the IPSec service. Here is the diagram for example above, knowing that some router models do not provide the capability to reroute ports within itself and two routers might be needed:



Here is a Linux Firewall configuration file when your VPN router does not provide the capability to reroute ports within itself and you want to add a front-end firewall:

firewall-reroute-port.sh

20.1.25 Is it possible to use Certificates from the Windows Certificate Store where our PKI software put user Certificates?

Yes. When setting up a new VPN Tunnel,

- Go to 'Phase1' > 'Certificate' tab
- All Certificates in the Windows Certificate Store (Personal Store) should appear here.
- Select the Certificate you need, click 'Ok', click 'Save'.

You might want to download our VPN Client software User Guide.

20.1.26 Is SHA-2 supported? Which Hash Algorithms are supported?

Yes. SHA-1 and SHA-2 256-bit are supported. MD5 is also supported. See full list in the datasheet.

20.1.27 How to see VPN Connections?

There are several ways to see opened VPN connections:

- Right click on the VPN Client software systray icon. Green lights mean VPN tunnels are open.
- Single click on the VPN Client software systray icon to open Configuration Panel. Tap Ctrl+Enter to go to Connection Panel, back and forth.
- Once the Configuration Panel pops up, click on 'Connections' button.

20.1.28 How to force all internet traffic in VPN tunnel?

It is possible to force all internet traffic in VPN tunnel. Doing so, all internet traffic is routed from the remote gateway instead of the remote user network, the remote user network IP address is virtually hidden to visited websites as it is replaced with remote gateway IP address. Corporate network may apply some additional traffic scan to increase security.

The VPN Configuration is simple and requires 3 steps:

- Go to 'Configuration Panel' > 'Parameters' > select 'Block non-ciphered connection' to prohibit non-ciphered traffic from being routed to internet directly.
- Go to 'Configuration Panel' > 'Phase2' > select 'Subnet Address' as 'Address Type' and set both 'Remote LAN' and 'Subet Mask' to '0.0.0.0', so that all traffic (to any IP address) will be routed to VPN tunnel. Note that '0.0.0.0' means all traffic including traffic to your local network will be routed through the VPN tunnel.
- On the remote gateway, set the VPN tunnel in the same way as both configuration must be symetrical with local subnet de 0.0.0.0/0. Note: this is only applicable to IPsec VPN gateway, this step is not required for SSL VPN tunnels.

Note: Some VPN Gateway/Routers may not support this feature (i.e. hub&spoke: '0.0.0.0/0'). If supported, you'll need to create a rule to authorize wan to wan traffic.

20.1.29 Does TheGreenBow VPN Client support WWAN?

Yes. WWAN stand for Wireless Wide Area Network or Wireless WAN, and now supported by several 3G/4G wireless modem/boards manufacturers. It uses mobile telecommunication cellular network technologies such as WIMAX, UMTS, GPRS, CDMA2000, GSM, HSDPA or 3G/4G to transfer data. WWAN connectivity allows a user with a laptop and a WWAN card to surf the web, check email, or connect to a virtual private network (VPN) from anywhere within the regional boundaries of cellular service.

Microsoft has introduced the WWAN miniport adapter to support it. The WWAN miniport adapter is used to manage establishment, configuration, packet transmission, packet reception and disconnection of NDIS-based data connections.

All manufacturers must support "Mobile Broadband Driver Model Specification" for Windows 7 based on NDIS6.20 miniport driver model. See our list of 3G modem/adapters.

20.1.30 How to disable the Gina feature?

In Windows Vista or Windows 7, the VPN Client might become unstable when restarting from Sleep or Hibernate mode. If you meet this problem, disabling "Gina mode" will fix this issue.

- Download those files to disable Gina in Windows Vista/Seven 32-bit or Gina in Windows Vista/Seven 64-bit
- Download those files to enable again>Gina in Windows Vista/Seven 32-bit or >Gina in Windows Vista/Seven 64-bit
- Once downloaded, double click to execute, click 'ok' to confirm.

20.2 Troubleshootings

"I have message XXXXX in the console". What does it mean?

We do make available for download a complete guide of messages from TheGreenBow VPN Client console with explanations and resolving hints. If this document does not help you, send us all the exchanges with RECV and SEND lines. Keep log levels to "0" and click on "Save file".
Log file can be found in C:\Program Files\TheGreenBow\TheGreenBow VPN.

No response from the VPN server

If you have the following logs, that means the remote VPN server does not answer to client's IKE requests.

```
115317 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
115319 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
115321 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
115323 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
```

Take a look at remote VPN server logs and check if requests from the client are received. If you find no trace, IKE requests must have been dropped somewhere. Check any firewall (including computer Personal Firewall) that can be found between the VPN Client and the VPN server.

VPN is up but I can't ping?

When logs look like the ones below, the IPSec VPN tunnel is established. Now you should be able to ping any devices onto your VPN server LAN. TheGreenBow VPN Client configuration is correct.

```
121902 Default (SA Cnx-Cnx-P2) SEND phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]
121905 Default (SA Cnx-Cnx-P2) RECV phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]
121905 Default (SA Cnx-Cnx-P2) SEND phase 2 Quick Mode [HASH]
```

If you still cannot ping the remote LAN, here are a few guidelines:

- Check Phase 2 settings : VPN client address and Remote LAN address. Usually, client IP address should not belong to the remote LAN subnet (read also What must be filled in Phase 2 field "VPN client address" ?)
- Once tunnel is up, packets are sent with ESP protocol. This protocol can be blocked by firewall. Check that every device between the client and the VPN server does accept ESP
- Check your VPN server logs. Packets can be dropped by one of its firewall rules.
- Check your ISP support ESP
- If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Ethereal for example). You will have an indication that encryption works.
- Check the "default gateway" value in VPN Server LAN. A target on your remote LAN can receive pings but does not answer because there is not "Default gateway" settings.
- You cannot access to the computers in the LAN by their name. You must have specified their IP address inside the LAN.

DELL or HP laptops with Broadcom Chipset

TheGreenBow recommends customers using a Broadcom chipset integrated with some Dell or HP laptops to update driver bcmwl5.sys to the most recent release. This driver causes blue screen intermittently even if our VPN Client is not installed.

Intel Adapter Switching Utility

Intel Adapter Switching Utility causes blue screen when TheGreenBow VPN Client is installed.
If you have an Intel Pro/Wireless 2100 or 2200, follow these steps in the given order.
Go to the Start/Control Panel/Add\Remove Programs. Remove the Intel PROset item
Go to the Start/Control Panel/System.
- Select the hardware tab and press the device manager button.
- In the device manager, click on the plus sign to expand the Network Adapters item.
- Select Intel PRO/Wireless LAN 2200 (or 2100) adapter and right click.
- Select Uninstall from the pop-up menu.

Restart the computer.

Upon reboot the laptop will re-detect the wireless card and install the drivers for it. It will not install the Intel PROset drivers. The wireless card should still function, but the added functionality of the adapter switching will not be available. Windows will then manage the wireless profiles instead of the Intel PROset utilities.

For more details, see the Intel technical advisory

I cannot uninstall VPN Client software

Problem: I cannot uninstall VPN Client software, it always asks to first uninstall the previous version.
Solution: You can use our tool to clean the remaining components of VPN Client software.

Issues with TheGreenBow drivers on Windows Vista

We strongly recommend users on Windows Vista to upgrade their network adapter drivers with Windows Update. This action can prevent from driver crashes in some network configurations. Also, Windows Vista bug fix pack KB938194 should be installed.
More details and download are available on http://support.microsoft.com/?kbid=938194.

Unable to open a VPN tunnel under Vista, problem with Vista Firewall?

Once TheGreenBow VPN Client installed on Vista, it might be impossible to open a VPN tunnel. The opening of the VPN tunnel remains blocked with the following IPSec messages (use the VPN Client console):

```
115317 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
115319 Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
```

This can happen on Windows Vista because the Vista Firewall can forbid IPSec communications.

TheGreenBow VPN IPSec 4.2 (and further): The software automatically creates new rules into the Windows Vista Firewall during software installation so that IPSec VPN traffic is enabled (see "windows firewall" in the User Guide).
Note: In Windows Seven (Wind 7), your profile 'Private' and 'Domain' in existing Windows Firewall rules for TheGreenBow VPN Client is not set accordingly. Please check in Windows Firewall rules and make sure your profile 'Private' and 'Domain' are selected (see step 6 below).
Restriction lifted in TheGreenBow VPN IPSec 4.7 (and further).

TheGreenBow VPN IPSec 4.1: To allow IPSec communications (or verify that they are authorized or restricted), please proceed as follows:

- Step 1: Go to 'Windows Start' button and enter "Windows Firewall with Advanced Security" in Search field. Alternatively, enter 'cmd' and in the command line window enter 'wf'.

- Step 2: Select in the left menu "Inbound Rules", then in the right column "New Rule...".

- Step 3: Select "Port" and then click on "Next".

- Step 4: Select "UDP" and the "Specific local ports," then enter two values 500 and 4500 separated by comma (i.e. "500,4500").
  Click on "Next".

- Step 5: Verify that "Allow the connection" bullet is selected.
  Click on "Next".

- Step 6: Make sure this rule applies to all Profiles. Click on "Next".

- Step 7: Assign a name to this new rule. Click on "Finish".

- Step 8: The new rule is created.

- Step 9: Select in the left column "Outbound Rules" and in the right column "New Rule...", and configure exactly the same rule (i.e. UDP ports 500 and 4500, VPN Outbound).

Purging driver cache under Windows Visa and Windows Seven

(VPN Client 4.* and 5.0)
In some cases, TheGreenBow NDIS driver may not be updated with a new software installation. For achieving this, follow the next steps :

- run "cmd.exe" as an administrator
- type "pnputil.exe -e" and press enter

The command output should be similar as :

```
Published name : oem68.inf
Driver package provider : Atheros Communications Inc.
Class : Network adapters
Driver version and date : 01/13/2009 7.6.1.204
Signer name : microsoft windows hardware compatibility publisher

Published name : oem86.inf
Driver package provider : TheGreenBow
Class : Network Service
Driver version and date : 05/19/2009 1.0.1.20
Signer name : thegreenbow

Published name : oem95.inf
Driver package provider : Microsoft
Class : Mobile devices
Driver version and date : 10/06/2004 4.0.4232.0
Signer name : microsoft windows hardware compatibility publisher

Published name : oem69.inf
Driver package provider : Acer
Class : Monitors
Driver version and date : 12/11/2006 1.00
Signer name : microsoft windows hardware compatibility publisher

Published name : oem78.inf
Driver package provider : Microsoft
Class : Network Service
Driver version and date : 01/24/2007 2.6.553.0
Signer name : microsoft windows hardware compatibility publisher
```

- find a "Driver package provider" line with "TheGreenBow" and note the INF file associated with. In our example, it is oem86.inf.
- type "pnputil.exe -d oem86.inf"

The driver should be entirely removed.

How to manually install VPN Client drivers?

(VPN Client 4.* and 5.0)

Microsoft Windows driver installation module might not install 3rd party drivers properly (e.g. TheGreenBow VPN Client ndistgb.inf drivers), especially when Windows is loaded with multiple tasks. Sometimes, registry settings are not performed properly, sometimes, not at all.

There is a simple manual procedure to get you up and running. The required drivers are still in the system, so no additional download should be necessary. Here are the steps:

- Go to Windows 'Configuation Panel' > 'Network and Sharing Center' > 'Manage Network Connections' > right click on a network connection > click on 'Properties'.

- Click on 'Install...'

- Select 'Service' and click on 'Add...'

- Click on 'Have Disk...' to find the drivers.

- Click on 'Browse...' to find the drivers.

- Go to C:\Program Files\Common Files\temp\{389b11eb-c24e-4a3d-8032-f44daa4cde4d} and select the 'ndistgb.inf' file (i.e. setup information), and click 'Open'.

- Proceed again with all other 'Network Connections' you want to use the VPN Client with.

VPN tunnel might fail to open after upgrade to Windows 8.1

VPN tunnel might fail to open after upgrade to Windows 8.1. Check if VPN Client console log shows the following message:

```
Default exchange_establish: transport "udp" for peer 'P1-P2' could not be created.
```

21. Contacts

Information and updates on TheGreenBow website: www.thegreenbow.com/vpn

Technical support by email: support@thegreenbow.com
or on TheGreenBow website: www.thegreenbow.com/support.html

Sales by email: sales@thegreenbow.com

22. Annex

22.1 Documentation reference

All documents referenced in this document can be downloaded on TheGreenBow website.

Document	Reference
TheGreenBow VPN Client Deployment Guide	tgbvpn_ug_deployment_en.pdf
TheGreenBow VPN Client Deployment Guide PKI Options	tgbvpn_ug_deployment_pki_en.pdf

22.2 Shortcuts

Connection Panel

- ESC close the window
- CTRL+ENTER Open the Configuration Panel (main window)

Configuration Panel VPN tree:

- F2 Edit the selected Phase
- DEL If a Phase selected, remove this Phase after user confirmation. If the whole VPN Configuration is selected (tree root), remove the whole configuration after user confirmation.
- CTRL+O If a Phase2 is selected, open the relevant tunnel.
- CTRL+W If a Phase2 is selected, close the relevant tunnel.
- CTRL+C Copy the selected phase in the clipboard.
- CTRL+V Paste the phase stored in the clipboard.
- CTRL+N If the VPN Configuration is selected, create a new Phase1. If a Phase1 is selected, create a new phase2 for this phase1.
- CTRL+S Save the VPN Security policy (VPN Configuration).

Configuration Panel

- CTRL+ENTER Switch to connection panel.
- CTRL+D Open the VPN « Console » window.
- CTRL+ALT+R Restart the IKE service.
- CTRL+ALT+D Activate the trace mode (logs).
- CTRL+S Save the VPN Security policy (VPN Configuration)..

22.3. List of available languages

Code	Langue	Nom français	Code ISO 639-2
1033 (default)	English	English	EN
1036	Français	French	FR
1034	Español	Spanish	ES
2070	Português	Portuguese	PT
1031	Deutsch	German	DE
1043	Nederlands	Dutch	NL
1040	Italiano	Italian	IT
2052	简化字	Chinese simplified	ZH
1060	Slovenscina	Slovenian	SL
1055	Türkçe	Turkish	TR
1045	Polski	Polish	PL

1032	ελληνικά	Greek	EL
1049	Русский	Russian	RU
1041	日本語	Japanese	JA
1035	Suomi	Finnish	FI
2074	српски језик	Serbian	SR
1054	ภาษาไทย	Thai	TH
1025	عـربي	Arabic	AR
1081	हिन्दी	Hindi	HI
1030	Danske	Danish	DK
1029	Český	Czech	CZ
1038	Magyar nyelv	Hungarian	HU
1044	Bokmål	Norwegian	NO
1065	ىفـارس	Farsi	FA
1042	한국어	Korean	KO

22.4. TheGreenBow VPN Client specifications

General	
Windows Versions	Windows 2000 32bit Windows XP 32bit SP3 Windows Server 2003 32bit Windows Server 2008 32/64bit Windows Vista 32/64bit Windows 7 32/64bit Windows 8 32/64bit
Languages	German, English, Arabic, Chinese (simplified), Korean, Spanish, Danish, Farsi, Finnish, French, Greek, Hindi, Hungarian, Italian, Japanese, Dutch, Norwegian, Polish, Portuguese, Russian, Serbian, Slovenian, Czech, Thai, Turkish
How to use General	
Invisible mode	Automatic opening of the tunnel upon traffic detection Access control to the VPN security policy Possible interfaces mask
USB mode	No more VPN security policy on the computer Opening of the tunnel when inserting a configured VPN USB key Automatic closing of the tunnel when extracting the configured VPN USB key
Gina	Opening of a tunnel before Windows logon Credential providers on Windows Vista, Windows 7 and further
Scripts	Running scripts configurable upon opening and closing of the VPN tunnel
Remote Desktop Sharing	Opening of a remote computer (remote desktop) with a single click through the VPN tunnel
Connection / Tunnel	
Connection mode	Peer-to-peer (point to point between two computers equipped with VPN Client) Peer-to-Gateway (see the list of qualified VPN gateways and their configuration guides)
Media	Ethernet, Dial up, DSL, Cable, WiFi Wireless LAN: GSM/GPRS, 3G, 4G

Tunneling Protocol	IKE based on OpenBSD 3.1 (ISAKMPD) Diffie-Hellmann DH Group 1 to 14 Full IPsec support
Tunnel mode	Main mode and Aggressive mode
Config mode	Network settings automatically retrieved from the VPN gateway
Cryptography	
Encryption	Symmetric: DES, 3DES, AES 128/192/256bit Asymmetric: RSA Diffie-Hellmann: DH group 1, 2, 5 and 14 (i.e. 768, 1024, 1536 and 2048bit) Hash: MD5, SHA-1, SHA-2 (SHA-256)
Authentication	Admin: Securing access to VPN security policies User: – X-Auth static or dynamic (request at each tunnel's opening) – Hybrid Authentication – Pre-shared key
PKI	– Certificates: support format X509, PKCS12, PEM – Multi-support: Windows certificate store, Smart card, Token – Certificates criteria: expiration, revocation, CRL, subject, key usage – Ability to select the Token / Smart card interface (see list of qualified Tokens / Smart card) – Automatic detection of Token / Smart card – Access to Token / Smart card in PKCS11 or CSP – Verification of "Client" and "Gateway" certificates
Miscellaneous	
NAT / NAT-Traversal	NAT-Traversal Draft 1 (enhanced), Draft 2, Draft 3 and RFC 3947, IP address emulation, includes support for: NAT_OA, NAT keepalive, NAT-T aggressive mode, NAT-T forced mode, automatic or off
DPD	RFC3706. Detection of non-active IKE end points.
Redundant Gateway	Management of a redundant gateway, automatically selected upon detection of DPD (inactive gateway)
Firewall	Filtering incoming / outgoing IP addresses and TCP / UDP ports
Administration	
Deployment	Options to deploy VPN policies (command line options for the set up, configurable initialization files...) Silent installation
VPN policies management	Options to import and export VPN policies Securing imports / exports by password, encryption and integrity monitoring
Automation	Open, close and monitor a tunnel from the command line (batch and scripts), startup and shutdown of software by batch file
Log and trace	IKE / IPsec logs console and trace mode activated
Live update	Checking for updates from the software
License and activation	Modularity of licenses (standard, temporary, limited duration), software activation (WAN, LAN), and deployment options (deployment of enabled software, silent activation...)

22.5. Credits and Licenses

Credits and license references.

/*
 * Copyright (c) 1998, 1999 Niels Provos. All rights reserved.
 * Copyright (c) 1998 Todd C. Miller <Todd.Miller@courtesan.com>. All rights reserved.
 * Copyright (c) 1998, 1999, 2000, 2001 Niklas Hallqvist. All rights reserved.
 * Copyright (c) 1999, 2000, 2001, 2002, 2004 Håkan Olsson. All rights reserved.
 * Copyright (c) 1999, 2000, 2001 Angelos D. Keromytis. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *   notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *   notice, this list of conditions and the following disclaimer in the
 *   documentation and/or other materials provided with the distribution.
 *
 * THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
 * IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
 * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
 * IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
 * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
 * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
 * THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
 * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
 * THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
 */

/* ==
 * Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *   notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *   notice, this list of conditions and the following disclaimer in
 *   the documentation and/or other materials provided with the
 *   distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *   software must display the following acknowledgment:
 *   "This product includes software developed by the OpenSSL Project
 *   for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *   endorse or promote products derived from this software without
 *   prior written permission. For written permission, please contact
 *   openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"

```
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
```

* 1. Redistributions of source code must retain the copyright
*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*   must display the following acknowledgement:
*   "This product includes cryptographic software written by
*   Eric Young (eay@cryptsoft.com)"
*   The word 'cryptographic' can be left out if the rouines from the library
*   being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*   the apps directory (application code) you must include an acknowledgement:
*   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/

Secure, Strong, Simple.

TheGreenBow Security Software